Date of Approval: January 27, 2017 PIA ID Number: **2099**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Identity Theft Tax Refund Fraud - Information Shar, IDTTRF - ISAC

2. Is this a new system? Yes

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**
Yes	**Detailed Design/Milestone 4A**
Yes	**System Development/Milestone 4B**
No	**System Deployment/Milestone 5**
No	**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.

This document addresses policies and procedures of a pilot of the Identity Theft Refund Fraud (IDTTRF) Information Sharing and Analysis Center (ISAC), which is a collaboration between IRS, states, and industry partners to combat identity theft. IRS participates in a unique role, which will not include any communications that identify individuals, while actively working with participants and aggregated data to reduce revenue losses due to fraud. Data elements are transmitted by the tax industry, providing information to strengthen the authentication that a tax return is being filed by the real taxpayer. As this effort is still in a pilot phase, the exact nature of the data exchange continues to develop. Some industry partners and/or states may take advantage of the ISAC host contractor's analysis by providing information about individuals from the returns they process. However, IRS will not have access to any of the information from the other partners before it is analyzed, aggregated, and individual identifiers are removed. It is expected that various State Departments of Revenue and tax industry companies will enroll as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. As of this time, membership is not finally determined as negotiations with potential members and new enrollment of members continues.

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.)? No

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**
No	**Date of Birth**	**No**	**No**	**No**
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**
No	**Tax Account Information**	**No**	**No**	**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

Selected	SBU Name	SBU Description
Yes	**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.**
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**
Yes	**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. The contractor may host information within the ISAC provided by the Industry and States to be used for analysis to identify patterns. This de-identified, anonymous data analysis will be shared with the ISAC partners.

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)**
No	**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.

This is a collaboration space designed for IRS, state revenue agencies, and industry to share information, therefore business contact information of ISAC partners such as email addresses and phone numbers will be listed for contact purposes. The ISAC provides a secure platform, to facilitate information sharing, consistent with applicable law, and analytics necessary to detect, prevent, and deter activities related to stolen identity tax refund fraud. Data elements are transmitted by the tax industry, providing information to strengthen the authentication that a tax return is being filed by the real taxpayer. All collection and use of SBU/PII in this environment is intended solely for the purpose of identifying and preventing refund fraud.

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

Each contributor of data utilizes a secured form of data transfer that includes accuracy verification checks in the transfer. Each partner/contributor is responsible for verifying the data in their environment prior to providing it to the contractor for analysis, distribution, or discussion, as applicable. Once on the ISAC, participants work to ensure that the information is applicable and valid prior to taking any action on it. This process does not bypass any individual taxpayer's right to due process related to any adverse actions.

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? Other

If **other,** explain your answer**.** Because no information in identifiable form is provided to the ISAC by IRS, there is no applicable Privacy Act System of Record Notice.

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? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? 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-Agenc Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Various (See narrative in Question 12c)	**Secure Data Transfer**	**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).

Organization Name	Transmission method	ISA/MOU

Various (See Narrative in Question 12e)	**Contractor**	**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? No

12b . Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? Yes

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

Organization Name	Transmission method	ISA/MOU
Various (see narrative)	**Secure Data Transfer**	**Yes**

Identify the authority and for what purpose? The ISAC Portal will post business contact information consisting of the name, email address, and telephone number of each member of the ISAC. No other PII material will be posted on the ISAC portal, per the Participant Agreement and Terms of Use Agreement. It is expected that various State Departments of Revenue and tax industry companies will enroll as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. As of this time, membership is not finally determined as negotiations with potential members and new enrollment of members continues.

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? Yes

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

Organization Name	Transmission method	ISA/MOU
MITRE	**Secure Data Transfer (SDT)**	**Yes**

Identify the authority and for what purpose? PII /SBU data is included in the ISAC, but is not provided or received by IRS, except as business contact information The ISAC Portal will post business contact information consisting of the name, email address, and telephone number of each member of the ISAC. PII material posted on the ISAC portal is secured according to the Participant Agreement and Terms of Use Agreement for each participant. In the Participant Agreement, in accordance with 26 CFR 301-7216-1(b)(2), all action, discussion, and sharing falls within the authority of the partner agencies to combat identity theft refund fraud. It is expected that various State Departments of Revenue and tax industry companies will enroll as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. As of this time, membership is not finally determined as negotiations with potential members and new enrollment of members continues.

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses? No

If **no**, explain. No Federal Tax Information will be contained on the site. Operating under Publication 4812 subject to IRS Review.

12e. Does this system disseminate SBU/PII to other Sources? Yes

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

Organization Name	Transmission method	ISA/MOU
Various ISAC Participants (see narrative)	**Contractor system**	**Yes**

Identify the authority and for what purpose? ISAC Participant Agreement. All action, discussion, and sharing falls within the authority of the partner agencies to combat identity theft refund fraud. It is expected that various State Departments of Revenue and tax industry companies will enroll as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. As of this time, membership is not finally determined as negotiations with potential members and new enrollment of members continues.

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?
Taxpayers receive required Privacy Act Notice during the process of interacting with the software providers. The taxpayers then provide detailed and personal information to industry partners in connection with their tax filing obligations. However, due to the nature of this ISAC, individual taxpayer may not receive specific notice that their return is under review unless and until it is selected and brought under a separate compliance program.

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):
All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as

Your Appeals Rights and How to Prepare a Protest. They can opt by choosing not to use that industry partner at all.

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

The ISAC does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this ISAC, individual taxpayers may not receive specific notice that their return is under review unless and until it is selected and brought under a separate compliance program. Industry Partner individual users of the ISAC sign a terms of use agreement that holds individuals accountable for violations of the rules of behavior.

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)

Contractor Owned and Operated

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

IRS Employees? No

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Each entity must sign the Participant's Agreement, signifying their agreement to the terms on behalf of their entity and their employees who will be accessing both the Collaboration and Sensitive Data sites. Each entity must identify a 'Trusted Point of Contact' to work with the contractor to establish user accounts for that entity. ONLY the trusted point of contact can recommend users for his/her entity. The contractor will only accept applications from the trusted point of contact. Once the trusted point of contact has been verified by the contractor Site Administrator, additional accounts for other users follow a process approved by contract. Once accounts are established, each person accessing the sites will be required to: Acknowledge/accept the 'Terms of Use' agreement Take the Rules of Behavior course and sign the certificate indicating the course has been completed. This is an annual mandatory security training course. Sign-on requires two-factor authentication. Users will be asked to create a 'secret' PIN to be used along with another message sent separately.

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? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

All records housed in the IDTTRF-ISAC are under the control of the ISAC contractor. It is not the IRS official repository for data and documents and does not require National Archives approval to affect data disposition. Output from the ISAC going to IRS will be managed using GRS 4.3, Item 030 and 031, System Documentation using GRS 3.1, Item 051, and Access and Audit Logs using GRS 3.2, Item 030. Any additional records developed from ISAC output and maintained by the IRS will be scheduled as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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. Though this is not an IRS system, with IRS documents, the contractor has assigned the contractor security representative to handle all security related systems and applicable security controls, per Publication 4812. IRS will have access for conducting Security Reviews.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. Because of the nature of the ISAC, it is more like a process than a system. The pilot will test the collaboration of the data, which is hosted on an established contractor platform that has been previously tested and secured, according to federal and FedRAMP classifications. A Contractor Site Review was completed the week of December 12, 2016. Results indicated approval by the sponsors, including IRS, with a final report due out in January 2017.

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: Not Applicable
26b. Contractors: Not Applicable

26c. Members of the Public: Not Applicable
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).
The volume of data on individuals is difficult to predict in the pilot stage. Any individual identifiers will be provided by the outside partners and not IRS. The purpose is to identify trends, not individuals.

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