Date of Approval: **March 17, 2021**

PIA ID Number: **5897**

SYSTEM DESCRIPTION

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

Identity Theft Tax Refund Fraud Information Sharing, IDTTRF-ISAC

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?

Identity Theft Tax Refund Fraud Information Sharing Analysis Center, IDTTRF-ISAC

What is the approval date of the most recent PCLIA?

5/12/2020

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

New Interagency Use

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.

IDTTRF-ISAC Senior Executive Board

Current ELC (Enterprise Life Cycle) Milestones:

Detailed Design/Milestone 4A

System Development/Milestone 4B

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.

In March 2015, the IRS convened a public-private partnership to respond to the growing threat of tax identity theft and stolen identity refund fraud. This group, called the IRS Security Summit, is made up of IRS officials, state tax administrators, and leading tax preparation firms, software developers, payroll and tax financial product processors, financial institutions, and tax professionals. In 2016, Security Summit partners agreed there was a need for a formal public-private partnership where sharing could take place in a collaborative environment based on partner-agreed rules which led to the formation of the Identity Theft Tax Refund Fraud (IDTTRF) Information Sharing Analysis Center (ISAC). The IDTTRF- ISAC has been recognized as a best practice for IRS, state tax agencies, and tax administration industry partners to combat tax refund identity theft. The term "online platform" is referring to the ISAC platform run by our Trusted Third Party (TTP). This document describes the unique role of the IRS in the collaboration. The Trusted Third Party (TTP) administers the ISAC by collecting partner data, de-identifying partner data when appropriate, analyzing the data, and then sharing the data and analytic products as appropriate with the partners. Data elements are transmitted by the tax industry, state tax agencies and the IRS providing information to strengthen the authentication that a tax return is being filed by the real taxpayer. As the fraud landscape changes the exact nature of the data exchange continues to evolve. Some industry partners and/or states utilize the ISAC host contractor's analysis by providing information from the returns they process. The ISAC "host contractor" is our Trusted Third Party (TTP). The IRS return information is housed in a separate secure enclave on the ISAC Platform. Pursuant to Taxpayer First Act (TFA) 2001-6103 (k)(14)- the Secretary may disclose specified return information to specified ISAC participants to the extent that the Secretary determines such disclosure is in furtherance of effective Federal tax administration relating to the detection or prevention of identity theft tax refund fraud, validation of taxpayer identity, authentication of taxpayer returns, or detection or prevention of cybersecurity threats.

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)

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

Pursuant to TFA 2001- 6103 (k)(14)- the Secretary may disclose specified return information to specified ISAC participants to the extent that the Secretary determines such disclosure is in furtherance of effective Federal tax administration relating to the detection or prevention of identity theft tax refund fraud.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed.

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
Internet Protocol Address (IP Address)
Financial Account Numbers
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.

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.

Proprietary data Business information that does not belong to the IRS.

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.

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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.

The host 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. Based on Participant Agreements signed by a partner and the Trusted Third Party, additional data elements may be shared. Item 6c- Additional Information- IRS does not share proprietary data to the ISAC. The Trusted Third Party, however, has proprietary information in connection with the ISAC such as its analyses, processes, software, techniques, technology, and tools.

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.

To comply with Taxpayer First Act (TFA) Section 6103(k)(14) the Secretary may disclose specified return information to specified ISAC participants to the extent that the Secretary determines such disclosure is in furtherance of effective Federal tax administration relating to the detection or prevention of identity theft tax refund fraud, validation of taxpayer identity, authentication of taxpayer returns, or detection or prevention of cybersecurity threats. The ISAC participants have access to a dynamic database of information used to identify trends and provide leads to thwart IDTTRF (Identity Theft Tax Refund Fraud) and other related activities, governed and secured by Participant Agreements with each entity. Therefore, business contact information of ISAC partners such as email addresses and phone numbers will be listed for contact purposes. The ISAC is now authorized to directly receive specified federal tax information (FTI) under IRC section 6103(k)(14) for the same purpose of identifying and thwarting IDTTRF. The IRS return information is housed in a separate secure enclave on the ISAC Platform. This FTI may include SSNs to the extent authorized by 6103(k)(14). All FTI shared and disseminated to and through the ISAC will be consistent with the purposes authorized by statute and used only as authorized by statute. Partners conduct training sessions within the secure ISAC platform to train fraud analysts. Training material provided by each partner (IRS, States, Industry) is marked as sensitive, as appropriate. All collection and use of SBU/PII in this environment are intended solely for the purpose of identifying and preventing refund fraud.

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

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.

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.

No

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: W&I RICS Return Review Program
Current PCLIA: Yes
Approval Date: 12/6/2019
SA&A: Yes
ATO/IATO Date: 5/22/2019

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)?

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).

Organization Name: Various State Agency ISAC Partners
Transmission Method: Secure Data Transfer
ISA/MOU: No

Does the system receive SBU/PII from other sources?

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: Various Industry ISAC Partners
Transmission Method: Secure Data Transfer
ISA/MOU: 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?

No

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

No

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

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: Various State Agency ISAC Partners
Transmission Method: ISAC Secure Platform
ISA/MOU: Yes

Identify the authority.

26 USC 6103

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

The ISAC is not a Federal system of records.

For what purpose?

PII material posted on the ISAC portal is secured according to the Participant Agreement. 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. State Departments of Revenue and tax industry companies are enrolled as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. A separate enclave in the IDTTRF-ISAC platform will receive and house IRS specified return information (FTI) provided under 6103(K)(14) and will distribute the FTI to the specified ISAC participants authorized to receive the return information for purpose of detection and prevention of identity theft tax refund fraud.

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

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: IRS
Transmission Method: ISAC Secure Platform
ISA/MOU: Yes

Identify the authority.

26 CFR 301-7216-1(b)(2), 26 USC 6103(k)(14)

For what purpose?

No

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

No

Explain:

The TTP receives return information under the authority of 6103(k)(14) not 6103(n). The TTP maintains confidentiality, safeguards and recordkeeping requirements consistent with 6103(k)(14) and the agreement entered into between the IRS and the TTP.

Does this system disseminate SBU/PII to other Sources?

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: Various Industry ISAC Partners
Transmission Method: ISAC Secure Platform
ISA/MOU: Yes

Identify the authority.

26 CFR 301-7216-1(b)(2) 26 USC 6103

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

The ISAC is not a Federal system of records.

For what purpose?

PII material posted on the ISAC portal is secured according to the Participant Agreement. 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. State Departments of Revenue and tax industry companies are enrolled as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. A separate enclave in the IDTTRF-ISAC platform will receive and house IRS specified return information (FTI) provided under 6103(K)(14) and will distribute the FTI to the specified ISAC participants authorized to receive the return information for purpose of detection and prevention of identity theft tax refund fraud.

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?

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.

PII material posted on the ISAC portal is secured according to the Participant Agreement. 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. State Departments of Revenue and tax industry companies are enrolled as members of the IDTTRF-ISAC and send/receive data to/from the ISAC. A separate enclave in the IDTTRF-ISAC platform will receive and house IRS specified return information (FTI) provided under 6103(K)(14) and will distribute the FTI to the specified ISAC participants authorized to receive the return information for purpose of detection and prevention of identity theft tax refund fraud.

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

No

Why not?

FTI is authorized to be disclosed by the IRS into the ISAC pursuant to section 6103(k)(14).

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Only

Managers: Read Only

IRS Contractor Employees

Contractor Users: Administrator

Contractor Managers: Administrator

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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

Section 6103(k)(14) specifies the authorized recipients of FTI. Agreements between the IRS and each authorized recipient detail the procedures for disclosing and disseminating FTI pursuant to section 6103(k) (14). 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 site 'Terms of Use', take the Security Training 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.

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.

IDTTRF-ISAC is non-recordkeeping and are under the control of the ISAC Trusted Third Party (TTP). 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 records generated and maintained by the IRS will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using already approved IRS Records Control Schedule (RCS), items for Tax administration and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. 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.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

3/30/2021

Describe 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. The Trusted Third-Party Authority To Operate infrastructure provides a consistently monitored environment that proactively identifies and addresses potential vulnerabilities, enabling partners to feel confident that their shared data is safe. The Trusted Third-Party security posture is maintained through security audits and compliance with the following standards - NIST 800-53 and IRS publication 4812 requirements.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The IDTTRF ISAC is subject to recurring IRS Contractor reviews in accordance with Publication 4812. The last 4812 completed report was in February 27,2020. The current 4812 review report is expected in the next two weeks. The Trusted Third Party's Authority To Operate infrastructure provides a consistently monitored environment that proactively identifies and addresses potential vulnerabilities, enabling partners to feel confident that their shared data is safe. The Trusted Third Party's security posture is maintained through security audits and compliance with the following standards - NIST 800-53 and IRS publication 4812 requirements.

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: Not Applicable

Contractors: Not Applicable

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

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

Tax return information is provided by some states as stated in the Participant Agreement signed by the Trusted Third Party, and the state. The volume of data on individuals varies based on the identified need of the state. The purpose is to identify trends, not individuals. IRS Records- the secure enclave in the ISAC for the specified return information (FTI) is operational, a rough estimate using last year’s data is over a million.

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