TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center

May 28, 2021

Report Number: 2021-25-025

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center

Final Audit Report issued on May 28, 2021 **Report Number 2021-25-025**

Why TIGTA Did This Audit

On July 1, 2019, Congress enacted the Taxpayer First Act and amended Code Section (§) 6103(k), *Disclosure of certain returns and return information for tax administration purposes,* to give the IRS the authority to disclose certain return information for the purpose of cybersecurity and the prevention of identity theft tax refund fraud. The IRS decided to leverage the Security Summit's Identity Theft Tax Refund Fraud Information Sharing and Analysis Center to disclose return information related to refund fraud schemes to State tax agencies and industry partners.

The overall objective of this review was to determine whether policies, procedures, and controls have been effectively implemented to ensure that disclosed return information is protected as required.

Impact on Taxpayers

The Security Summit's primary mission is to assist in the fight against the filing of fraudulent tax returns and protect taxpayers from identity theft tax refund fraud. Ensuring the protection of shared return information from unauthorized disclosure allows the IRS and the Security Summit to leverage all available resources to further reduce identity theft tax refund fraud.

What TIGTA Found

In March 2020, the IRS signed a memorandum of understanding with the [redacted] Corporation, the contractor who operates and manages the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center, to facilitate the disclosure of and access to specified return information under the authority of Code § 6103(k)(14). The memorandum of understanding is the primary control document for the IRS to share its Federal tax information with the contractor and industry partners.

The IRS and the contractor generally ensured that their actions complied with the law for sharing Federal tax information. This included addressing privacy controls, ensuring that the contractor securely received and stored shared data and monitored its use, and ensuring use of two-factor authentication to identify and authenticate individuals who access the shared data.

However, additional policies, procedures, and actions are needed to improve the effectiveness of security over the sharing and storing of the data. Specifically, while Federal tax information is transmitted through secure connections, TIGTA found [redacted]

In addition, opportunities exist to enhance controls and ensure consistency in applying policies for accessing the shared data. Lastly, the Information Sharing and Analysis Center alternate processing site does not meet the filing season maximum tolerable downtime to avoid unacceptable delays.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that [redacted] are timely remediated; the Commissioner, Wage and Investment Division, and the Chief Privacy Officer, where applicable, enhance controls to ensure consistency in applying policies for accessing the shared Federal tax information; and the Commissioner, Wage and Investment Division, ensure that the contractor's alternate processing site is converted to [redacted] that meets the maximum tolerable downtime.

The IRS agreed with all of our recommendations. The IRS plans to ensure that vulnerabilities identified on the servers are updated and remediated, perform the annual tabletop exercise and provide the incident information as required, update the Privacy and Civil Liberties Impact Assessment, and incrementally increase the alternate processing site toward a [redacted] categorization.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 28, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (Audit # 202020510)

This report presents the results of our review to determine whether policies, procedures, and controls have been effectively implemented to ensure that disclosed return information is protected as required. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix III.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

In recognition of the escalating challenges facing tax ecosystems, Internal Revenue Service (IRS) officials with representatives from the State Departments of Revenue, the Chief Executive Officers of leading tax preparation firms, software developers, and payroll and tax financial product processors came together to form the Security Summit. The Security Summit's primary mission is to assist in the fight against the filing of fraudulent tax returns and protect taxpayers from identity theft tax refund fraud. An initiative of the Security Summit was to share refund schemes, which resulted in the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center, hereafter referred to as the ISAC. The IRS launched the ISAC as a pilot on January 23, 2017. According to the IRS, it is a [redacted][1] operated by the [redacted] Corporation for the purpose of detecting, deterring, and preventing tax-related identity theft.

Through an existing contract, the IRS tasked [redacted] to create and maintain the ISAC, which is a platform housed in a [redacted] owned environment. The ISAC was designed to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information. [redacted] is also responsible for ensuring the ISAC site's reliability and security. The IRS views the ISAC as an essential tool for collecting and quickly sharing meaningful identity theft tax refund fraud schemes among the member organizations.

The ISAC stakeholders, which include IRS leadership and its partners who operate the ISAC, are illustrated in Figure 1 below.

Figure 1: [redacted]

[1] See Appendix IV for a glossary of terms.

During [redacted] development and implementation of the ISAC in January 2017, the IRS's oversight activities ensured adherence to data protection and privacy requirements. Executives from the Wage and Investment (W&I) Division's Return Integrity and Compliance Services (RICS) function partnered with the Privacy, Governmental Liaison and Disclosure (PGLD) office, and the Office of Chief Counsel to obtain input on the ISAC's implementation plans as they related to data protection and privacy and to help ensure that applicable requirements were followed. The PGLD office led the IRS team in working with [redacted] to complete a Privacy and Civil Liberties Impact Assessment (PCLIA). This assessment helped to ensure that the data shared in the ISAC would conform to applicable data protection statutes and meet IRS disclosure, privacy, safeguard, and security policy and standards. Through the assessment, the PGLD office identified that the data elements collected by the ISAC during its pilot year would contain data categorized as Personally Identifiable Information and Sensitive But Unclassified, but would not contain Federal tax information (FTI).

On July 1, 2019, Congress amended Code § 6103(k)[2] by enacting the Taxpayer First Act (TFA).[3] The TFA gave the IRS the authority to disclose certain return information for the purpose of cybersecurity and the prevention of identity theft tax refund fraud. Specifically, § 2003 of the TFA provides that the Secretary of the Treasury, hereafter referred to as the Secretary, *may disclose specified return information to designated ISAC Participants[4] 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.*

Briefly, the process to become an ISAC participant, *i.e.,* entity/organization, with access to FTI is as follows.

- The IRS authorizes[5] the entity/organization to be a member of the Security Summit. Prior to authorization, the entity/organization has to qualify, which includes filing returns or representing a specific market segment. Next, the entity/organization enters into a signed ISAC Participant Agreement with [redacted], hereafter referred to as the Trusted Third Party (TTP), which enables them to access the secure ISAC portal.[6]
- The entity/organization has access to FTI by entering into a written agreement in the form of a memorandum of understanding. The IRS provides the list of the authorized ISAC participants to the TTP relative to the operational aspects of sharing FTI. As of December 2020, there were 73 ISAC participants.
- The TTP sends a notification to the entity/organization's trusted point of contact to identify users who can access FTI. As of December 2020, there were 427 ISAC users, of which 125 (29 percent) had access to FTI. The TTP works directly with each authorized entity/organization/user to create and delete user access.
- Once the individual users electronically complete the TTP FTI Use Rules, which includes a reminder of the users' agreement with the IRS regarding their use, safeguards and

[2] 26 U.S.C. § 6103(k), *Disclosure of certain returns and return information for tax administration purposes*.

[3] Public Law 116–25, 133 Stat. 981 (2019).

[4] For purposes of this report, the terms ISAC participants and ISAC partnerships are used interchangeably.

[5] The W&I Division's RICS function is responsible for the Security Summit and ISAC programs.

[6] An entity/organization official and the TTP Contracting Officer sign the ISAC Participant Agreement.

incident reporting obligations as well as their responsibility for reporting unauthorized accesses, they are given access to FTI. The TTP maintains the list of individual ISAC users.

Results of Review

On March 3, 2020, the IRS signed a memorandum of understanding with the TTP to facilitate the disclosure of and access to specified return information under the authority of Code § 6103(k)(14) *Disclosure of Return Information for Purposes of Cybersecurity and the Prevention of Identity Theft Tax Refund Fraud.* The memorandum of understanding is the primary control document for the IRS to share its FTI with the TTP and industry partners.

The IRS and the Trusted Third Party Generally Complied With the Taxpayer First Act for Sharing Federal Tax Information

The memoranda of understanding complied with the TFA

We found the memorandum of understanding for sharing FTI with the ISAC complied with the TFA. The TFA includes provisions that specify the return information that can be disclosed; restrictions on the use of the disclosed information; and data protections and safeguards. We identified 26 stipulations in the TFA.

- In 21 of the 26 stipulations, there were little to no differences between the TFA and the memorandum of understanding. The stipulations included 12 related to specifying the return information that can be disclosed, seven related to restrictions on the use of the disclosed information, and two related to data protections and safeguards.
- The remaining five stipulations were not included in the memorandum of understanding because they were applicable only to the IRS and not the TTP. These included four germane to return information that can be disclosed and one to data protection and safeguards.

We also reviewed the memorandum of understanding between the IRS and each of the 14 industry partners permitted to receive FTI for compliance to the law.[7] We identified similar compliance with 20 of the 26 TFA stipulations. The remaining six stipulations were not applicable to the industry partners because they included specifying return information that could be disclosed and the IRS does not disclose return information directly to the industry partners. Instead, it is obtained from the TTP.

Privacy controls were addressed

The memorandum of understanding with the TTP requires the adherence to Publication 4812, *Contractor Security & Privacy Controls*, including an Annual Contractor Site Security Assessment. We observed this assessment in February 2020 and noted repeat issues to which we obtained an approved risk-based decision document and a flaw remediation issue for which the IRS provided

[7] The States are governed under 26 U.S.C. § 6103(d) *Disclosure to State tax officials and State and local law enforcement agencies* regarding the sharing of FTI and do not require a separate memorandum of understanding.

a valid explanation. We also noted an alternate processing site requirement issue, which we address later in this report.

The TTP's employees are required to take Privacy Awareness Training. We noted that the Cybersecurity team's assessment of the training showed the TTP met the requirement and that the contracting officer representative provided written documentation certifying the completed training. Separate from the memorandum of understanding, the TTP requires similar privacy awareness training which is included in the rules of behavior for users who have access to the ISAC to analyze partners' sensitive information and share analytic results. If the rules are not acknowledged and dated, the users cannot obtain access to the sensitive information. Because we obtained access to the ISAC, we participated in the initial and annual training and concluded that the process was working as intended.

We also reviewed a privacy related notification for users who access FTI on the ISAC Participant Area landing page. The notification included a warning that the system is for authorized use and the consequences, which included disciplinary and civil and criminal actions for unauthorized and improper use. The notification further warned that users should have no reasonable expectation of privacy regarding any communication or data transiting or stored on the system. In addition, the ISAC is not a Federal system of records and is not required to comply with the Privacy Act.[8]

The IRS disclosed specified return information in accordance with the TFA

The TFA outlines the data elements that the IRS is allowed to share with the ISAC for potential and confirmed identity theft tax refund fraud cases. For potential identity theft tax refund fraud cases, the IRS can share eight data related fields from electronically filed tax returns.[9]

- The Internet Protocol address.
- The device identification.
- The e-mail domain name.
- The speed of completion.
- The method of authentication.
- The refund method.
- Other return information related to the electronic filing characteristics of such returns as the Secretary may identify.
- A return prepared by a tax preparer to include the Preparer Taxpayer Identification Number and the electronic filer identification number.

For confirmed identity theft refund fraud cases, the IRS can share an additional four data fields.

- The name of the taxpayer as it appears on the return.
- The Taxpayer Identification Number of the taxpayer as it appears on the return.

[8] 5 U.S.C. § 552a.

[9] The IRS stated it shares data elements from paper-filed returns, too. However, we did not review the data elements from paper returns.

- The bank account information provided for making a refund.
- The bank routing information provided for making a refund.

The IRS currently shares [redacted] information files with the TTP: a [redacted] potential identity theft refund fraud file, a [redacted] confirmed identity theft refund fraud file, and [redacted] confirmed identity theft refund fraud file. Between April and May 2021, the IRS plans to make available a [redacted] containing the [redacted] confirmed [redacted] identity theft refund fraud data. This file will have data fields similar to the [redacted] confirmed refund fraud file. We analyzed the April 24, 2020, [redacted] potential identity theft refund fraud file, the June 2020 [redacted] confirmed identity theft refund fraud file, and the Calendar Year 2019 [redacted] confirmed identity theft refund fraud file. We determined that the data fields shared by the IRS with the ISAC contained only the specified return information in accordance with the TFA.

The TTP securely received and stored FTI and monitored its use

The memorandum of understanding requires the TTP to maintain a [redacted]. We found that the TTP took measures to ensure the separation of FTI and non-FTI. [redacted] We verified that the TTP maintains FTI on [redacted] by comparing a list of the files that we received from the IRS to the designated ISAC accounts.

The stored and transmitted FTI also includes appropriate encryption to protect against unauthorized access and viewing. In addition, the TTP monitors ISAC activities by performing weekly automated reviews and monthly manual reviews to ensure that only authorized users have accessed the ISAC.

Disclosure and re-disclosure of FTI were properly captured and provided to the IRS

The memorandum of understanding requires the TTP to maintain a record of all re-disclosures and provide the IRS a monthly accounting of the re-disclosures within [redacted] of the close of each month. Transmitting FTI to the TTP is considered a permitted disclosure. [redacted] it is considered a re-disclosure, which the memorandum of understanding between the IRS and the TTP permits.

We verified that the TTP is providing the IRS with a monthly accounting of the re-disclosures. The TTP reported more [redacted][10] [redacted]

Two-factor authentication is used to identify and authenticate individuals who access FTI

Publication 4812 requires the use of two-factor authentication for system access. Two-factor authentication requires the use of 1) something a user knows (such as a password) and 2) something a user possesses (such as a token card) to access the contractor's information

[10] In [redacted] the IRS began sharing FTI with the TTP, one month after signing the memorandum of understanding with the TTP.

system. We reviewed the latest updated version of the ISAC System Security Plan, which included the use of two-factor authentication, and found no security issues with this control. We also confirmed that the TTP is using two-factor authentication when we used something we knew and something we possessed to independently access the ISAC portal.

While the IRS and the TTP generally ensured that its actions complied with the TFA for sharing FTI, additional policies, procedures and actions are needed to improve the effectiveness of security over the sharing and storing of FTI. Specifically,

- FTI are transmitted through secure connections; however, [redacted]
- Opportunities exist to enhance controls and to ensure consistency in applying the policies for accessing FTI.
- The ISAC alternate processing site does not meet the filing season maximum tolerable downtime to avoid unacceptable delays.

The purpose of the ISAC is to provide a secure platform via a sustainable public/private partnership and to facilitate information sharing on activities related to identity theft tax refund fraud. Securing servers that store FTI prior to transmission to the TTP; updating procedures and applying consistent policies for those who access FTI; and ensuring continuity of operations in the event of a disaster provides the IRS and the TTP with an opportunity to better achieve the ISAC's purpose in a secure manner.

Federal Tax Information Is Transmitted Through Secure Connections; However, [redacted]

We determined the connections that the IRS used for transmitting FTI to the TTP were secure. Specifically, the IRS is using the [redacted] approved by the National Institute of Standards and Technology in Special Publication 800-52 Revision 2 (August 2019), *Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations*, and no known protocol vulnerabilities were identified related to the connections. We also reviewed for security vulnerabilities on the IRS servers housing FTI prior to transmission.[11] On August 31, 2020, during our audit work, the IRS switched vulnerability scanning tools from [redacted] Therefore, we are presenting the results for each scanning tool.

[11] The IRS places [redacted]

[redacted] scan results

Our review of the IRS's [redacted] vulnerability scans from March through June 2020 identified [redacted]

We identified [redacted]

[redacted] The policy further states that remediation begins when a vulnerability is discovered.

Figure 2 lists the number of [redacted][12]

Figure 2: [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Source: Our analysis of IRS [redacted] reports of [redacted] scan results from March 20, 2020, through June 12, 2020.

When we shared the results of our analyses with IRS personnel, the IRS explained that some of the vulnerabilities were a result of the [redacted], *i.e.*, the software installation was not complete. It further stated that the [redacted] software was misconfigured for the two backup servers, but the [redacted]. However, we also identified vulnerabilities other than the [redacted] findings that resided on the servers, such as the [redacted] The IRS further stated that it patches monthly and that the [redacted] IRS personnel also stated that the scans are run [redacted] now; however, at the time of our audit work, they ran the [redacted] scans twice a week.

[12] For the vulnerabilities without a discovered date because of their age, we used the publication date generated by the Common Vulnerabilities and Exposure Editorial Board.

To verify whether the identified vulnerabilities were resolved, we reviewed [redacted] scans dated August 17, 2020, through August 20, 2020, and confirmed that the vulnerabilities attributed to the same [redacted] had been corrected for the two production servers that stored FTI for transmission to the TTP. However, we found [redacted] were the same as the ones we previously found that had resided on the [redacted] The remaining [redacted] were identified in July 2020 on a [redacted] Figure 3 reflects our follow-up analysis of [redacted]

Figure 3: [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Source: Our follow-up analysis of IRS [redacted] reports of [redacted] scan results from August 17, 2020, through August 20, 2020.

[redacted] scan results

Our review of the IRS's [redacted] vulnerability scans from August 17, 2020, through September 18, 2020, identified [redacted]

- [redacted]
- [redacted]

The IRS stated that it decided to use the [redacted] vulnerability scanning tool because it was able to increase network coverage, improve reporting times, and reduce the need to perform remote credentialed vulnerability scans by incorporating an agent. In addition, IRS personnel felt the [redacted] tool was more robust and found it to be more accurate in reporting vulnerability findings. For example, the [redacted] tool continuously picked-up on remnants or computing footprints of older versions of software when upgrades occurred. [redacted], on the other hand, understands when upgrades occur and disregards those remnants or footprints when evaluating vulnerabilities. In addition, [redacted] accounts for service packs that might cover multiple patches, thus reporting that those related vulnerabilities have been addressed. We were unable to verify the differences and effectiveness between the two vulnerability scanning tools. However, both [redacted] and [redacted] scan results throughout the audit continued to show the existence of [redacted]

Unresolved [redacted] that remain on [redacted] may unnecessarily expose the server to exploitation and compromise. Foreign cyber actors continue to exploit publicly known and older software vulnerabilities against public and private sector organizations. We found that [redacted] By focusing remediation efforts on the highest scoring vulnerabilities, the IRS can achieve the greatest possible risk reduction to the FTI stored on the servers for transmission to the TTP.

Recommendation 1: The Chief Information Officer should ensure that the appropriate updates are installed to timely remediate the [redacted]

Management's Response: The IRS agreed with the recommendation. Enterprise Operations will ensure that the [redacted] are updated and remediated by installing the appropriate updates.

Office of Audit Comment: The IRS's corrective action does not fully address the recommendation, as it relates to the "timely" remediation of the [redacted] The IRS's security patch management policy specifically outlines when [redacted] should be remediated.

Controls and Policies Over Accessing Federal Tax Information Need Improvement

As previously discussed, the IRS and the TTP established controls that complied with the TFA to secure FTI. However, we did identify some controls that need updating and some policies regarding access that need to be consistently applied to FTI.

We identified controls that need to be updated and policies regarding access that need to be consistently applied to FTI.

The memorandum of understanding between the IRS and the TTP needs updating regarding incident reporting

Incident reporting was not aligned with internal guidance to include the CSIRC as one of the primary points of contact

The CSIRC serves as the primary coordination point for incident response within the IRS. It oversees all incident-reporting activities at the IRS, and it serves as the liaison between the IRS and the Department of the Treasury's Government Security Operations Center for all communications and follow-up activities in response to an activity. The IRS is required to report breaches or incidents, whether confirmed or suspected, to the Government Security Operations Center as quickly as possible after discovery in no more than one business day.

The memorandum of understanding, Exhibit D, *Incident Reporting Procedures*, requires the TTP to report any incident/situation in accordance with its existing ISAC contract with the IRS,

consistent with [redacted][13] [redacted]

As a comparison, Publication 4812 names the CSIRC as part of the incident reporting control. Specifically, it requires all incidents related to IRS processing, information, or information systems to be reported within one hour to the contracting officer representative and security incidents shall be reported to the CSIRC by contacting the CSIRC Support Desk. In addition, [redacted]

We reviewed the tabletop exercise[14] that the TTP performed in July 2019 and July 2020. The primary objectives of the exercise were to:

- Validate the [redacted]
- [redacted] incident response handling and reporting procedures.
- Identify areas of the incident response plan that need to be revised.

We confirmed that the TTP reported the security incident to TIGTA, the contracting officer representative, and the Office of Safeguards as part of the simulation activity. However, the tabletop exercise document did not show that the simulated incident was reported to the CSIRC.

Because the CSIRC is the primary IRS function to respond to security incidents and coordinate reactive and preventative actions from incidents across the enterprise, it is imperative that it is aware of all incidents directed at IRS's assets, including those at IRS third-party systems to ensure that appropriate actions are taken.

The incident response table top exercise neither tested nor reported all aspects of responding to an incident

Exhibit D in the memorandum of understanding requires the TTP to report any possible improper inspection or disclosure of return information, including breaches and incidents, to TIGTA immediately, but no later than 24 hours after identification of a possible issue. In addition, it requires notification by e-mail to the Office of Safeguards. The notification, via a data incident report, is to consist of documentation of the specifics of the incident or breach known at that time and includes the following items.

- Name of the TTP and point of contact for resolving the data incident.
- Date, time, and address when/where the incident occurred and was discovered.
- Description of the incident, the data involved, and how the incident was discovered.
- Potential number of FTI records involved.

[13] [redacted]

[14] The title of the exercise (*i.e.*, test) is [redacted] Incidence Response Test and Exercise but it is referred to as the tabletop exercise training.

- Information Technology assets involved (*e.g.,* laptop, server, mainframe).

During our review of the tabletop exercise training document, it did not show that the TTP generated a simulated report with the required data fields, such as the data involved and the potential number of FTI records involved. A TTP official confirmed that the TTP did not test whether the necessary data could be produced as required by Exhibit D. The IRS stated that a report can be generated for the Fiscal Year 2021 Incident Response exercise and the report will be available for review.

We requested the TTP provide a limited report showing the FTI filename, date, and the type of files (*i.e.,* potential or confirmed identity theft tax refund fraud) that the ISAC users downloaded during March 2020 to July 2020. The TTP provided a report listing the date and file type, but did not provide the filename. The TTP stated that providing the filename would require a manual review of each FTI file name and would entail some anonymization. We believe that using a manual process to identify the filename of the files that the users download could create a delay in reporting this information to the IRS and TIGTA, which could subsequently delay the reporting and investigation into possible unauthorized disclosure incidents.

Our review of the requested information showed that 31 industry partner users downloaded 155 files[15] from the ISAC. Of the 155 files downloaded, 137 files were the IRS's FTI files consisting of 102 potential identity theft tax refund fraud files and 35 confirmed identity theft tax refund fraud files. The confirmed files contained Personally Identifiable Information, *i.e.,* the taxpayer's name, Social Security Number, bank account number, and bank routing number. Because the TTP did not provide the filenames that were downloaded, we could not determine whether a [redacted] or [redacted] confirmed identity theft refund fraud file was downloaded. Without the filenames, we could not calculate the precise number of taxpayer records in the files.

The W&I Division's RICS function stated it is currently coordinating with the PGLD office on Exhibit D in the memorandum of understanding and will ensure that both the exhibit and standard operating procedures have the same language as Publication 4812, so that all required IRS offices are informed of a security incident within the required time frames (specifically, CSIRC will be notified). In addition, incident response reporting will be included in future tabletop exercises conducted by the TTP.

The privacy notification was not fully completed for all privacy aspects

As mentioned previously, the IRS completed a PCLIA for the ISAC to ensure that the data shared conforms to applicable data protection and privacy standards. The IRS requires system owners to update PCLIAs every three years or sooner if there are major changes to the systems. The existing PCLIA for the ISAC is dated December 18, 2019, and was not updated after Congress's July 2019 approval to permit the sharing of FTI. However, during our audit work, the IRS's PGLD office and the W&I Division's RICS function worked with the TTP to update the PCLIA, which was approved May 12, 2020.

We reviewed the latest PCLIA and found that the IRS appropriately completed most sections in the PCLIA, which contained 31 questions that require a response, with the exception of two sections.

[15] Each file contains more than one taxpayer account.

- One section (6.c) asked, *Does this system contain sensitive but unclassified information that is not Personally Identifiable Information, it uses, collects, receives, displays, stores, maintains, or disseminates?* The IRS answered "no" for "Proprietary data" that is defined as *Business information that does not belong to the IRS.* We found the ISAC [redacted]
- The second section (21) asked, *The following people have access to the system with the specified rights: IRS Employees? No.* In addition, the table indicating the access levels (read only, read-write, or administrator) for each type of IRS employee, *i.e.,* users, managers, administrators, or system developers, was left blank. We found IRS employees do have access to the ISAC with various access levels. As of December 2020, 87 IRS employees were users, 31 had access to FTI, including TIGTA employees (audit and investigations) who are provided access to the ISAC as IRS users.

We provided our findings to the PGLD office; it collaborated with the W&I Division's RICS function and determined that the PCLIA was accurate and no changes were necessary. The IRS stated it completed the PCLIA specifically to the IRS as an ISAC participant. Specifically, in response to the PCLIA questions:

- For section (6.c), the IRS stated it does not provide any proprietary data to the ISAC. An example of proprietary business data (which does not belong to the IRS) would be business information that the IRS collects during a taxpayer audit to determine audit issues. The IRS is not sharing this type of data with the ISAC. Sensitive but unclassified information owned/provided by ISAC industry partners and the contractor are not subject to Federal Government agency definitions and rules. Regardless of the information they may contribute to the ISAC, it cannot fall under the definition of sensitive but unclassified, because a Federal agency does not own or maintain it.
- For question (21), the table is blank because the question – under the Information Protection section of the PCLIA – pertains to the owner/operator of the system, which is not the IRS. To interpret the question in the context of Information Protection by the contractor owner/operator of the ISAC platform, it is asking about the contractor's employees who have administrative access and manage the ISAC platform. Whereas, IRS employees have limited access to only their own folder on the ISAC as an ISAC participant, not as a system administrator.

We disagree with the IRS's decision that no changes are needed. Using the Participant Agreement between the TTP and ISAC participant and the IRS's definition of a PCLIA, the TTP is the system owner. Therefore, the PCLIA should reflect the owner's analyses and descriptions of the ISAC system and the information that is being collected, *e.g.,* the nature and source; the intended use of the information, *e.g.,* to verify existing data; and to whom the information will be shared with (not specifically to the IRS, although the IRS is a participant). The ISAC and the TTP, operating on behalf of the ISAC, is a tax return preparer governed by Code § 7216. The ISAC collects information from the IRS, the States, and its industry partners for assisting with detecting and preventing identity theft tax refund fraud. It uses the data to conduct analysis studies and to convey the results for the purposes of the ISAC. The TTP considers all data provided and its analyses of the data as sensitive information to ensure the privacy, security, and

confidentiality of the data. [redacted] In addition, the fact that IRS employees have access to their folders in the ISAC supports that they have at least read-only capabilities to their own folders. There is other information in the ISAC that IRS employees can access that is not related to FTI, *i.e.,* [redacted]

The IRS states on its website that it recognizes the importance of protecting the privacy and civil liberties of taxpayers and uses the PCLIA as the vehicle for addressing privacy and civil liberty issues in a system. The PCLIA demonstrates that program/project managers, system owners, and developers have consciously incorporated privacy and civil liberty protections throughout the entire system. When the PCLIA is inaccurate and incomplete, it weakens the assurances that it was designed to promote. After sharing our disagreement and request for the IRS to reconsider its decision, the IRS stated it still contends that its response to the proprietary data section is accurate; however, it recognized the importance of assurances that privacy and civil liberty protections remain throughout the system and agreed to make the changes to the PCLIA.

The Commissioner, W&I Division, should:

Recommendation 2: Update Exhibit D, *Incident Reporting Procedures*, in the memorandum of understanding between the IRS and the TTP by adding the CSIRC function as another primary point of contact to ensure that the TTP properly reports incidents/situations.

> **Management's Response:** The IRS agreed with the recommendation. On February 2, 2021, the IRS updated Exhibit D, *Incident Reporting Procedures*, in the memorandum of understanding between the IRS and the TTP, by adding the Computer Security Incident Response Center function as another primary point of contact to ensure that the TTP properly reports incidents/situations.

Recommendation 3: Ensure that the TTP updates the tabletop exercise training to include the required data fields, *i.e.,* the filename of data involved and the potential number of FTI records involved, and test whether the incident information can be produced as required by Exhibit D, *Incident Reporting Procedures,* in the memorandum of understanding between the IRS and the TTP.

> **Management's Response:** The IRS agreed with the recommendation. The TTP will perform the annual tabletop exercise and provide the incident information as required by Exhibit D, *Incident Reporting Procedures*.

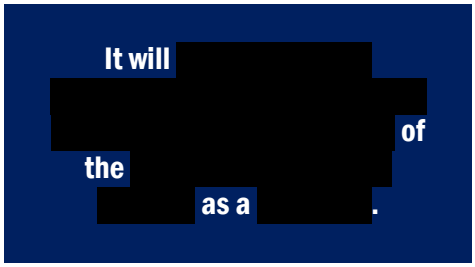
The Commissioner, W&I Division, and the Chief, Privacy Officer, should:

Recommendation 4: Coordinate with the TTP to ensure that the PCLIA is updated to correctly reflect that the [redacted] and that IRS employees have access to the data in the ISAC and their access level.

> **Management's Response:** The IRS agreed with the recommendation. The Privacy and Civil Liberties Impact Assessment will be updated to correctly reflect that [redacted] and that IRS employees have access to the data in the ISAC and their access level.

The Information Sharing and Analysis Center Alternate Processing Site Does Not Meet the Filing Season Maximum Tolerable Downtime

According to the *Alternate Processing Site* section in Publication 4812, alternate processing sites are geographically distinct from primary processing sites. In addition, the publication requires that the contractor ensure that the equipment and supplies required to resume operations at the alternate site are in place, or that required equipment/supplies are made available within specified time frames to avoid unacceptable delays in the delivery of contracted services. The information technology, personnel, and physical security controls shall be commensurate with the sensitivity of the information being restored and with the security of the original processing site.



Guidance from the National Institute of Standards and Technology's Special Publication 800-34 Revision 1 (May 2010), *Contingency Planning Guide for Federal Information Systems*, states that an organization should ensure that equipment, supplies, and pertinent agreements are in place to support delivery of primary processing capabilities to an alternate site within specified time frames to avoid unacceptable delays should the primary processing capabilities become unavailable. Further, the alternate processing site should provide information security safeguards that are equivalent to those of the primary site. The guidelines further describe three common categorizations for alternate processing sites: cold, warm, or hot sites.

- Cold sites are locations that have the basic infrastructure and environmental controls available (*e.g.*, electrical and heating, ventilation and air conditioning), but with no equipment or telecommunications established or in place. There is sufficient room to house equipment needed to sustain a system's critical functions.
- Warm sites are locations that have the basic infrastructure of cold sites, but also have sufficient computer and telecommunications equipment installed and available to operate the system at the site. However, the equipment is not loaded with the software or data required to operate the system.
- Hot sites are locations with fully operational equipment and the capacity to quickly take over system operations after loss of the primary system facility. A hot site has sufficient equipment and the most current version of production software installed and adequate storage for the production system data. Hot sites should have the most recent version of backed-up data loaded, requiring only updating with data since the last backup.

The ISAC business process owners collaborated on the potential impact of a loss of the process/service and agreed that the maximum tolerable downtime the process owners and users are willing to accept is as follows:

- [redacted]
- [redacted]

We reviewed the October 1, 2019, draft alternate processing site plan for the ISAC to determine the resources needed to build an alternate processing site. According to the plan, the TTP determined that the ISAC classifies as a moderate-impact system based on Federal Information

Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*. The plan also included a detailed cost summary to build a replica of the [redacted] as an alternate processing option based on the inventory of current resources required to operate. The detailed cost summary estimates a cost of [redacted] of the [redacted] as a [redacted]

In response to the need for an alternate processing site identified during the Publication 4812 review of the ISAC in February 2020, the TTP developed an alternate processing site strategy and implemented a "no cost" [redacted] The TTP is committed to working with the IRS to incrementally "warm" the site.

However, our review of the current and future alternate processing site choices found that neither meets the maximum tolerable downtime needs for a filing season. The IRS responded that ongoing discussions continue between it and the TTP, considering the costs and benefits associated with increasing resources and maintenance for a [redacted] When asked whether the IRS considered establishing a [redacted] within an IRS building or computing center, the TTP responded [redacted]

The ISAC is an important platform for the IRS and its partners' day-to-day operations to combat identity theft tax refund fraud and gain near term data on emerging trends, and its continuity of operations is critical to ensure that fraud information is timely shared with its partners. The IRS found that the ISAC directly protected about $3 million in fraudulent identity-theft Federal refunds from being issued during Calendar Year 2018. Its importance will only continue to grow over time.

Recommendation 5: The Commissioner, W&I Division, should ensure that the ISAC alternate processing site is converted to a [redacted] that achieves the maximum tolerable downtime to prevent any filing season delays.

Management's Response: The IRS agreed with the recommendation. The TTP and IRS are incrementally increasing the alternate processing site toward a [redacted] categorization.

Office of Audit Comment: The IRS's corrective action, which is planned to be implemented in approximately three years, does not provide sufficient information regarding how it plans to incrementally increase the alternate processing site toward becoming a [redacted] and address the filing season maximum tolerable downtime of 24 hours.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether policies, procedures, and controls have been effectively implemented to ensure that disclosed return information is protected as required. To accomplish our objective, we:

- Interviewed key stakeholders from the IRS's W&I Division, PGLD, and Information Technology offices, and the TTP to gain an understanding of the ISAC roles and responsibilities, and the policies, procedures, and processes over the handling of FTI.
- Evaluated the IRS's memoranda of understanding to determine whether the procedures and guidelines for sharing FTI with the ISAC and the industry partners complied with the TFA § 2003.
- Analyzed the April 24, 2020, [redacted] potential; June 2020 [redacted] confirmed; and the Calendar Year 2019 [redacted] confirmed identity theft tax refund fraud files shared by the IRS with the ISAC to determine whether the data contained only the specified return information in accordance with the TFA § 2003.
- Reviewed required privacy documents and notifications, such as the PCLIA, to determine whether the documents and notifications were properly updated to incorporate the sharing of FTI with the ISAC.
- Evaluated the IRS and TTP's network architecture to determine whether data transfer connections were protected with end-to-end transmission encryption as well as data-at-rest encryption, [redacted] were available to receive and store FTI separate from non-FTI, and two-factor authentication was used to restrict logical access to FTI.
- Reviewed [redacted] vulnerability scans from March through June 2020 and August 17, 2020, through August 20, 2020, and [redacted] vulnerability scans from August through September 2020, to identify any [redacted] on hardware or software of network components related to the [redacted]
- Followed-up on the February 2020 IRS Annual Cybersecurity Contractor Security Assessment's unresolved findings that included issues on flaw remediation and an alternate processing site needed to be geographically distinct from the primary ISAC processing site in case of a disaster to determine whether the issues have been resolved.

Performance of This Review

This review was performed at the TTP office in [redacted], and with information obtained from the W&I Division's Accounts Management and RICS functions located in Atlanta, Georgia; the Information Technology organization's Cybersecurity function located in Lanham, Maryland; and the PGLD office, Chief Counsel office and Office of Professional Responsibility located in Washington, D.C., during the period March 2020 through January 2021. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Kent Sagara, Director; Deborah Smallwood, Audit Manager; Cindy Harris, Lead Auditor; George Franklin, Senior Auditor; and Thomas Martin, Information Technology Specialist.

Validity and Reliability of Data From Computer-Based Systems

During this review, the Cybersecurity function provided four [redacted] data files of [redacted] Vulnerability scans [redacted] We evaluated the data by (1) confirming that the data fell within the time frames requested; (2) ensuring supporting evidence confirmed that the data files were authenticated and credentialed when scanned; and (3) interviewing Cybersecurity function personnel on their processes and procedures on conducting vulnerability assessments for risk assessment and compliance purposes. Based on these results, we believe that the data used in our review were reliable for the purposes of this report.

We also used five confirmed identity theft files (the June, July, August, and September 2020 [redacted] files and the Calendar Year 2019 [redacted] file issued in June 2020) transmitted to the TTP using the previously mentioned servers. The file transmissions occurred from June 9, 2020, through September 23, 2020. We verified the record count of each of the files downloaded from the ISAC to a disclosure report the TTP prepared using a TIGTA interface data analysis program to ensure that all of the records were downloaded. We also analyzed the confirmed identity theft refund fraud data shared by the IRS with the ISAC by comparing it with the TFA and determined that the data contained only the specified return information, *i.e.,* the taxpayer names and Taxpayer Identification Numbers, in accordance with the TFA. Based on these results, we believe that the data used in our review were reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the compliance with the TFA of the memoranda of understanding between the IRS and the TTP and the IRS and the industry partners; IRS privacy and security policies and procedures; disclosure laws; the National Institute of Standards and Technology guidance; and the TTP security controls for the protection of FTI transmitted and stored in systems. We evaluated these controls by interviewing IRS and TTP personnel responsible for the security and operations of the ISAC, conducting a site visit to the TTP location, reviewing transmitted data files, and reviewing relevant documentation.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective action will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 634,314 unique taxpayers whose Personally Identifiable Information, including banking information, was transmitted in the confirmed identity theft files that were temporarily stored on the IRS servers (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

By reviewing the IRS's [redacted] reports of [redacted] scan results for the period March 20, 2020, through June 12, 2020, we identified [redacted] We found [redacted]

We reviewed the five confirmed identity theft files (the June, July, August, and September 2020 [redacted] files and the Calendar Year 2019 [redacted] file issued in June 2020) transmitted to the TTP using the servers. The file transmissions occurred from June 9, 2020, through September 23, 2020, the date the IRS stated it corrected the vulnerabilities. The files contained 634,314 unique taxpayers with Personally Identifiable Information, *i.e.,* the name of the taxpayer, Social Security Number, bank account number, bank routing number, and Internet Protocol address.

Appendix III

Management's Response to the Draft Report

COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

April 16, 2021

MEMORANDUM FOR MICHAEL E MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin David P. Alito Digitally signed by David P. Alito Date: 2021.04.19 15:55:21 -04'00'
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (Audit # 202020510)

Thank you for the opportunity to review the draft audit report and provide comments. The creation of the Information Sharing and Analysis Center (ISAC) was an initiative undertaken by the IRS in 2017 as a means by which to share among the IRS, state Departments of Revenue, and trusted industry partners, observations and trends involving tax-related identity theft fraud schemes. The ISAC is designed to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information. Enactment of the Taxpayer First Act (TFA) in 2019 expanded our ability to share more detailed information about suspicious and confirmed identity theft with the ISAC participants. The enhanced information assists the alliance in detecting and preventing refund fraud with a broader information source on the threat of identity theft and risk. We appreciate your acknowledgement of our compliance with the TFA requirements and the implementation of appropriate restrictions on the sharing of federal tax information. The restrictions were incorporated into the Trusted Third Party (TTP) agreement with ISAC participants and establish the guidelines to safeguard and secure the data stored in the ISAC.

The security of the shared return information within the ISAC will continue to be protected and available to assist Security Summit partners with their detection efforts. As the information is used and shared within the ISAC, we will continue to ensure that its security is always a priority. We recognize the importance of constant improvement in identifying tax refund fraud schemes and protecting revenue within the tax ecosystem. Any expansion of information shared by the IRS is carefully evaluated to ensure alignment with disclosure and security guidelines. We continue to strengthen our controls and procedures by updating the Incident Reporting Procedures to include the Computer Security Incident Response Center function in our processes; requesting the

perform an annual tabletop exercise; and updating our Privacy and Civil Liberties Impact Assessment to correctly reflect that the ISAC includes [redacted] and that IRS employees have access. We will continue to work with the TTP to qualify the alternate processing site as a [redacted] under the National Institute of Standards and Technology's Special Publication 800-34 Revision 1 (May 2010), *Contingency Planning Guide for Federal Information Systems* during the filing season.

We will evaluate the recommendations and implement them as noted. We believe the amount of federal tax information shared with the ISAC community will only increase over time and will continue to benefit our external partners in combatting tax-related identity theft fraud. The success of the ISAC will continue to improve collectively as each entity identifies and detects fraudulent tax returns.

We agree with the outcome measures. Our responses to your specific recommendations are enclosed. If you have any questions, please contact me, or a member of your staff may contact Michael Beebe, Director, Return Integrity and Compliance Services, Wage and Investment Division, at 470-639-3250.

Attachment

Attachment

Recommendation

RECOMMENDATION 1
The Chief Information Officer should ensure that the appropriate updates are installed to timely remediate the [redacted]

CORRECTIVE ACTION

Enterprise Operations will ensure that the [redacted] are updated and remediated by installing the appropriate updates.

IMPLEMENTATION DATE
June 15, 2021

RESPONSIBLE OFFICIAL
Associate Chief Information Officer, Enterprise Operations, Information Technology

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management system of controls.

Recommendations

The Commissioner, W&I Division, should:

RECOMMENDATION 2
Update Exhibit D, Incident Reporting Procedures, in the memorandum of understanding between the IRS and the TTP by adding the CSIRC function as another primary point of contact to ensure that the TTP properly reports incidents/situations.

CORRECTIVE ACTION

On February 2, 2021, the IRS updated Exhibit D, *Incident Reporting Procedures*, in the memorandum of understanding between the IRS and the TTP, by adding the Computer Security Incident Response Center function as another primary point of contact to ensure that the TTP properly reports incidents/situations.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification Program Management, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Ensure that the TTP updates the tabletop exercise training to include the required data fields, i.e., the filename of data involved and the potential number of FTI records involved, and test whether the incident information can be produced as required by Exhibit D, *Incident Reporting Procedures*, in the memorandum of understanding between the IRS and the TTP.

CORRECTIVE ACTION

The TTP will perform the annual tabletop exercise and provide the incident information as required by Exhibit D, *Incident Reporting Procedures*.

IMPLEMENTATION DATE
April 15, 2022

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification Program Management, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management system of controls.

Recommendation

The Commissioner, W&I Division, and the Chief, Privacy Officer, should:

RECOMMENDATION 4
Coordinate with the TTP to ensure that the PCLIA is updated to correctly reflect that the [redacted] and that IRS employees have access to the data in the ISAC and their access level.

CORRECTIVE ACTION

The Privacy and Civil Liberties Impact Assessment will be updated to correctly reflect that [redacted] and that IRS employees have access to the data in the ISAC and their access level.

IMPLEMENTATION DATE
July 15, 2021

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification Program Management, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management system of controls.

Recommendation

RECOMMENDATION 5
The Commissioner, W&I Division, should ensure that the ISAC alternate processing site is converted to a [redacted] that achieves the maximum tolerable downtime to prevent any filing season delays.

CORRECTIVE ACTION

The TTP and IRS are incrementally increasing the alternate processing site toward a [redacted] categorization.

IMPLEMENTATION DATE
April 15, 2024

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification Program Management, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management system of controls.

Appendix IV

Glossary of Terms

Term	Definition
Agent (in the context of the [redacted] Vulnerability scanning tool)	A lightweight program installed locally on a laptop, virtual system, desktop, and/or server. Agents perform scans locally, and report vulnerability, compliance, and system results back to the central server.
Alerts	Issued by members within the ISAC's secure environment to report any tax ecosystem threats. This is like a neighborhood listserv for the tax ecosystem, with immediate reports of breaches, compromised identification numbers, or other suspect data.
Anonymization	The use of one or more techniques designed to make it impossible – or at least more difficult – to identify a particular individual from stored data related to them. The purpose of data anonymization is to protect the privacy of the individual and to make it legal for governments and businesses to share their data without getting permission.
Common Vulnerabilities and Exposure Editorial Board	The Board, which is sponsored by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, makes content decisions regarding discovered vulnerabilities. The Board has a membership that includes information security specialists from commercial security-tool vendors, government agencies, and academic/research institutions.
[redacted]	[redacted]
Federal tax information	Consists of Federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
[redacted]	A [redacted]-owned environment intended to meet strategic needs for partnership-driven, secure data analytics at scale. It creates an agile, efficient, and scalable platform for hosting projects, including the ISAC.
ISAC Participant Agreement	An agreement between the TTP and the ISAC participant's entity/organization that includes data sharing guidelines, data submission protocols, ownership and uses of data, and data security and protection.
ISAC Participant Area	An area in the ISAC to access FTI and reports, *etc.* Access to this area requires the completion of annual ISAC security and rules of behavior training.
[redacted]	[redacted]
Landing page	The section of a website accessed by clicking a hyperlink on another web page, typically the website's home page.

Term	Definition
[redacted] Corporation	A private, independent, not-for-profit organization, chartered to work in the public's interest. [redacted] has set up ISACs for the health industry (which, like the IRS, has laws requiring protection of sensitive data) and for the airline industry and has prior technological expertise in building ISACs.
[redacted]	[redacted]
Publication 4812, *Contractor Security & Privacy Controls*	Designed to identify security requirements for contractors and any subcontractors supporting the primary contract. It identifies security controls and privacy requirements for contractors (and their subcontractors) who handle or manage IRS sensitive but unclassified information on or from their own information systems or resources.
[redacted]	[redacted]
Service pack	An orderable or downloadable update to a customer's software that fixes existing problems and, in some cases, delivers product enhancements.
[redacted]	[redacted]
Tabletop exercise training	The incidence response tabletop exercise brings members of the incidence response team together to simulate their response to a security and privacy incidental scenario(s). It is a cost-effective and efficient way to identify gaps, overlaps, and discrepancies in the incidence response handling capabilities.
Tax ecosystem	Taking a holistic look at the entire tax system, from the end-user workstation to filing the tax return and beyond.
[redacted]	A vulnerability scanner product that uses the Common Vulnerabilities and Exposures architecture to cross-link between compliant security tools and describes individual threats and potential attacks.
[redacted]	A vulnerability scanner product used to monitor systems for extraneous services or insecure settings that are exploitable. Each system is given a score based on how well the applicable hardening guidelines are implemented. Systems that score lower than the acceptable quality level or are found to contain high-risk settings are updated to rectify the insecure settings and reduce risk of exposure.
Trusted point of contact	This person is the single point of contact between an ISAC entity/organization and the TTP for the purposes of creating or removing user access to the ISAC portal.

Appendix V

Abbreviations

CSIRC	Computer Security Incident Response Center
FTI	Federal Tax Information
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISAC	Identity Theft Tax Refund Fraud Information Sharing and Analysis Center
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison and Disclosure
RICS	Return Integrity and Compliance Services
TFA	Taxpayer First Act
TIGTA	Treasury Inspector General for Tax Administration
TTP	Trusted Third Party
W&I	Wage and Investment

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.