The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed

September 28, 2017

Reference Number: 2017-20-064

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

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

1-800-366-4484

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.

THE IDENTITY THEFT TAX REFUND FRAUD INFORMATION SHARING AND ANALYSIS CENTER GENERALLY ADHERED TO DATA PROTECTION STANDARDS, BUT ADDITIONAL ACTIONS ARE NEEDED

Highlights

Final Report issued on September 28, 2017

Highlights of Reference Number: 2017-20-064 to the Internal Revenue Service Deputy Commissioner for Operations Support and Deputy Commissioner for Services and Enforcement.

IMPACT ON TAXPAYERS

The IRS issues more than $400 billion in refunds and processes more than 240 million tax returns and other forms each year. As such, the IRS is a target for identity thieves and cyber criminals. In January 2017, the IRS stood up the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (hereafter referred to as ISAC) to provide a secure platform for sharing identity theft tax refund fraud information among the IRS, State tax agencies, and the private industry tax sector. The IRS views this ISAC as an essential tool for collecting and quickly sharing meaningful identity theft tax refund fraud schemes among the member organizations and reducing the risk to taxpayers.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS developed the ISAC in accordance with Federal security standards to ensure that sensitive fraud data are protected against unauthorized access. The IRS contracted with an external private organization to create and maintain this ISAC and ensure the site's reliability and security.

On September 30, 2016, the Information Sharing and Analysis Organization Standards Organization published voluntary standards and guidelines for use by emerging and established Information Sharing and Analysis Centers. The IRS also requires its contractors to implement security and privacy controls in accordance with Publication 4812, *Contractor Security Controls*, when handling or managing IRS sensitive information.

WHAT TIGTA FOUND

The IRS's oversight of its contractor ensured that data protection and privacy requirements were generally adhered to during the development and implementation of the ISAC. To determine compliance with Publication 4812, the IRS conducted its initial contractor security assessment in December 2016 before the ISAC went live to ensure that proper security and privacy management controls were in place. However, the physical security portion of the contractor security assessment was not performed, leaving the status of some controls unknown.

During the course of our review, the contractor was still working to implement and improve some required controls, including the implementation of certain security controls, a privacy incident response plan, a risk assessment, flaw remediation policy and procedures, and improvement of its plan of action and milestones processes.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS ensure that the contractor completes implementation of all required security controls, including a privacy incident response plan, a risk assessment, and timely flaw remediation, and improves the plan of action and milestones process. In addition, the IRS should conduct the physical security portion of the contractor security assessment and ensure that physical security deficiencies are corrected in a timely manner.

The IRS agreed with our recommendations. The IRS plans to monitor progress and ensure implementation of required controls. The IRS completed the physical security controls portion of the contractor security assessment and through contract monitoring plans to ensure that corrective actions are implemented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 28, 2017

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT
DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed (Audit # 201720006)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) developed the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center in accordance with Federal security standards to ensure that sensitive fraud data are protected against unauthorized access. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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

Abbreviations

CSA	Contractor Security Assessment
DNS	Domain Name System
****2*****	**********2**********
FMSS	Facilities Management and Security Services
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
NIST	National Institute of Standards and Technology
PGLD	Privacy, Governmental Liaison, and Disclosure
POA&M	Plan of Action and Milestones

Background

The importance of information sharing to data security has been discussed for well over a decade. Early realization of its importance led to the creation of Information Sharing and Analysis Centers (ISAC) for critical U.S. infrastructures to ensure the protection of information systems and the physical assets supporting them. In May 1998, Presidential Decision Directive 63[1] directed public-private partnerships in specific sectors to create ISACs as a means to share information about threats, warning of attacks, and actual attacks on critical Government and private sector infrastructures.

Early realization of the importance of information sharing to data security led to the creation of Information Sharing and Analysis Centers.

In February 2015, Presidential Executive Order 13691[2] directed the Department of Homeland Security to encourage the development of Information Sharing and Analysis Organizations (ISAO) to enable effective and near real-time sharing of cyber risks and incidents. On September 30, 2016, the ISAO Standards Organization[3] published voluntary standards and guidelines for use by emerging and established ISAOs.[4] These publications were developed in response to Presidential Executive Order 13691 to promote robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.

The Internal Revenue Service (IRS) issues more than $400 billion in refunds and processes more than 240 million tax returns and other forms each year.[5] As a result, the IRS has become a target for identity thieves to steal extremely valuable tax information and for cyber criminals to file falsified tax returns to get fraudulent refunds. To help combat this growing problem, in March 2015, the IRS Commissioner convened a Security Summit meeting of public and private tax administration leaders to discuss the evolving threat posed by increasingly sophisticated identity thieves and ways to leverage their collective resources and efforts. In 2016, one of the

[1] Presidential Decision Directive 63, *Critical Infrastructure Protection: Sector Coordinators* (May 22, 1998).
[2] Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (February 13, 2015).
[3] Through an open and competitive process, the Department of Homeland Security selected the University of Texas at San Antonio as the non-government organization to identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs. Led by the University of Texas at San Antonio, the ISAO Standards Organization was established October 1, 2015.
[4] ISAOs and ISACs are trusted entities established by their membership to provide comprehensive all-hazards analysis that is shared within the sector, within a profession, across a particular community of interest, with other sectors, and with the Federal Government. ISAOs may provide their membership with risk mitigation, incident response, and alert and information sharing. The goal is to provide users with accurate, actionable, and relevant information.
[5] IRS, *Management's Discussion and Analysis, Fiscal Year 2016*.

initiatives that resulted from the Security Summit was to create an Identity Theft Tax Refund Fraud ISAC (hereafter referred to as ISAC)[6] that would provide a secure platform for sharing identity theft tax refund fraud information among the IRS, State tax agencies, and the private industry tax sector.

Through an existing contract, the IRS tasked the****2***[7] *****2*** (hereafter referred to as ***2***) to create and maintain the ISAC, which is a web-based platform housed in a ***2***-owned environment.[8] ***2*** stated that the ISAC is designed to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information. ***2*** is also responsible to ensure 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 IRS indicated that the ongoing collaboration between the IRS, State tax agencies, and private industry tax sector stakeholders is critical to combatting identity theft tax refund fraud and reducing the risk to taxpayers.

The ISAC pilot became operational in January 2017. Following its initial deployment, the IRS stated that it would work with the ISAC members to assess the ISAC's value and effectiveness. The IRS expects that future iterations of the ISAC will include additional data sets that will enhance identity theft detection and prevention and provide greater capabilities for data analytics.[9] The IRS plans the ISAC to have full operational capabilities by Calendar Year 2019.

Currently, the ISAC provides two levels of access for its participants.

1. The alerts and rapid response collaboration space. Alerts contain information related to new identity theft schemes or other threats to the tax ecosystem. The goal of alerts is to enable members to proactively identify potential fraudulent activity. Details provided in an alert may include information related to what schemes have been identified, indicators of suspicious activity, and types of accounts targeted. Alerts may also include anecdotal evidence from ISAC members who have already been targeted by this scheme.
2. The leads and other sensitive data site for data analytics and data visualization. Leads contain data derived from research and analysis performed by the tax industry partners on tax returns and provide identity theft data to the IRS and the States. This reporting is

[6] The IRS's full name for its ISAC is the "Identity Theft Tax Refund Fraud ISAC." For conciseness, we will use "ISAC" in this report when referring to the IRS's ISAC.

[7]**********2**********2**********2**********2**********.

[8]**********2**********2**********2**********2**********.

[9] For the first year, the IRS indicated that no taxpayer information will be shared in the ISAC.

done in accordance with IRS authorized e-filer providers' responsibilities under Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* and State operating agreements.

As of May 2017, the IRS reported that the ISAC has 39 member organizations that collectively have submitted a total of 1,794,049 industry leads and posted 34 alerts in support of combating identity theft refund fraud. The IRS indicated that the sharing helps to create awareness and conversation around current schemes and activities related to identity theft refund fraud across the tax ecosystem and will encourage members to share best practices related to identity theft prevention and detection.

This review was performed at **********2********** **********2*******, and with information obtained from the IRS Offices of Criminal Investigation; Privacy, Governmental Liaison, and Disclosure (PGLD); Cybersecurity; and the Wage and Investment Division located in New Carrollton, Maryland, during the period November 2016 through June 2017. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Information Sharing and Analysis Center Generally Adhered to Data Protection Standards

During ****2*** development and implementation of the ISAC, the IRS's oversight activities ensured adherence to data protection and privacy requirements.[10] The IRS ISAC Executive Official is from Criminal Investigation. The Wage and Investment Division's Return Integrity and Compliance Services organization is administering the contract with ***2***. These organizations partnered with the PGLD organization and the Office of Chief Counsel to obtain their 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 organization led the IRS team in working with ***2*** to complete a Privacy and Civil Liberties Impact Assessment. 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 organization 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.

In regards to system security and privacy controls, the ISAO Standards and Guidelines, issued by the Department of Homeland Security, provide the minimum levels of security that should be considered when establishing an ISAC. These basic ISAO security standards include:

- **Secure Communications** – Data-at-rest and the data-in-transit are adequately protected and include appropriate encryption.
- **Access Controls** – Appropriate controls are in place so people are allowed access to only information they are authorized to access.

[10] Applicable data protection and privacy requirements included: the Privacy Act of 1974, 5 U.S.C. § 552a (2013); the Consolidated Appropriations Act, Public Law 114-113, which included at Division N, Title I the Cybersecurity Information Sharing Act of 2015 (2016); National Institute of Standards and Technology (NIST), Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (Apr. 2010); NIST, Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013); ISAO Standards Organization, ISAO 300-1, *Introduction to Information Sharing*, v1.0 (Sep. 2016); and IRS Publication 4812, *Contractor Security Controls*.

- **Cybersecurity Attack and Data Breach Notification** – Internal reporting plans and communication lines with members are established in the event they are a victim of a cybersecurity attack.
- **Data Classification, Distribution, and Labeling** – Adequate policy and procedures are in place to appropriately mark and label information for proper handling.
- **Member Security** – Adequate policy and procedures are in place for ensuring that members have signed agreements regarding their responsibilities for securing the shared information and training members on their responsibilities.

We determined that ****2*** successfully implemented minimum controls in accordance with ISAO standards that included: 1) secure communication mechanisms to prevent unauthorized disclosure and modification of ISAC information; 2) adequate access control policy and procedures that met Federal requirements, including the use of two-factor authentication to identify, authorize, and authenticate individuals for accessing ISAC systems; 3) adequate monitoring of system use; and 4) detailed tracking mechanisms to ensure that appropriate member agreements (including the ISAC Participant Agreement, Terms of Usage Agreement, and the Rules of Behavior) are in place and participants are trained on data security prior to system access. In addition, ***2*** has included appropriate privacy information on the ISAC site entry page to ensure that participants are aware of their privacy rights and responsibilities.

Further, ***2*** is working to implement privacy and security controls in accordance with IRS Publication 4812, *Contractor Security Controls*, which the IRS requires when contractors handle or manage IRS sensitive but unclassified information,[11] including Federal tax information. While, as previously mentioned, the IRS is not sharing Federal tax information in the ISAC during its pilot year, that may change in the future. The IRS indicated that, following the pilot year, it plans to work with ISAC members to assess the ISAC's value and effectiveness. In addition, future iterations of the ISAC could include additional data sets, such as Federal tax information, intended to enhance identity theft detection and prevention. Therefore, should the IRS decide to include tax return information in the ISAC in the future, ***2*** would be on track to have the appropriate privacy and security controls in place.

While Most Applicable Security Controls Were Implemented, Some Were Still Planned or Needed Improvement

Publication 4812 defines the basic security controls, requirements, and standards for protecting IRS data and applies to contractors, contractor employees, and any subcontractors supporting the primary contract. Publication 4812 is based on the National Institute of Standards and

[11] IRS sensitive but unclassified information includes all taxpayer returns and return information, as defined by Internal Revenue Code Section 6103; all Personally Identifiable Information in which there is information that can be associated to a specific individual; and other sensitive information.

Technology (NIST) Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*.[12]

To determine compliance with Publication 4812, the IRS conducts an annual on-site contractor security assessment (CSA) for all contracts subject to this publication. Publication 4812 provides the framework and general processes for conducting the CSAs, through which the IRS monitors compliance and assesses the effectiveness of the required security controls. The CSAs cannot be a self-assessment performed by the contractor.

The IRS Cybersecurity Security Risk Management, Security Controls Test and Evaluation, CSA office conducted an initial on-site CSA of ***2**** ISAC from December 13, 2016, to December 16, 2016, in*****2**********, to ensure that proper security and privacy management controls were in place. At that time, the ISAC was still under development and did not contain any data.

During its December 2016 review, the CSA team identified findings on 33 (17 percent) out of 193 security and privacy control tests based on Publication 4812 requirements. ***2*** recorded its actions, or planned actions, to correct or address all 33 findings in Plan of Action and Milestones (POA&M) and in the ISAC System Security Plan. The CSA team will verify whether ****2*** corrections were effective when they conduct their next assessment in July 2017. As of June 2017, ***2*** indicated to the IRS that only 14 remained open, and that eight would be closed by July 2017.

While ***2*** is working to implement all required controls, we are highlighting the following seven issues for IRS's attention.

- *********2**********.
- *********2**********.
- Privacy Incident Response Plan.
- Risk Assessment.
- Flaw Remediation Policy and Procedures.

[12] The E-Government Act of 2002 (Public Law 107-347), Title III, Federal Information Security Management Act of 2002 (Pub. L. No. 107-347, Title III, 116 Stat. 2899, (2002) (codified as amended in 44 U.S.C. §§ 3541-3549) (2013)), as amended by the Federal Information Security Modernization Act of 2014 (Public Law 113-283), requires each agency to provide security for "the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." To ensure Federal Information Security Management Act compliance, the NIST identifies specific security controls and criteria in NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. While NIST Special Publication 800-53 Rev. 4 is a general guide, the intent of Publication 4812 is to provide IRS security requirements in the IRS contracting environment.

- POA&M processes.
- Physical Security Review.

The first four controls listed have planned completion dates in the future, extending to December 2017. We believe the IRS should verify that ****2*** corrective action plans are adequate for these controls and that each remain on track for completion. We found that the next two controls, related to flaw remediation and corrective action plans, needed improvements to achieve full implementation. Last, the physical security portion of the CSA has not yet been performed.

**********2**********

**********2**********.[13] **********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********[14]**********.

**********2**********

**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********.

[13] Office of Management and Budget Memorandum 08-23, *Securing the Federal Government's Domain Name System Infrastructure* (August 22, 2008).
[14] Cache poisoning, also called DNS poisoning or DNS cache poisoning, is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address.

Privacy Incident Response Plan was still under development

Publication 4812 requires the contractor to develop and implement a Privacy Incident Response Plan that provides an organized and effective response to privacy incidents, including reporting such incidents within one hour to the appropriate IRS officials. While ***2*** had an incident response plan for its overall environment, it did not have a Privacy Incident Response Plan in place specifically for the ISAC. ****2**** indicated that the ISAC Privacy Incident Response Plan required changes from the existing overall environment incident response plan. ***2*** expected those changes to be complete by July 2017.

Without a Privacy Incident Response Plan, privacy-related incidents may not be reported in a timely manner to appropriate IRS officials to allow for a quick response to any potential security incident or unauthorized disclosure.

A risk assessment of the harm that could result from unauthorized access was not conducted

Publication 4812 requires, for all information systems environments, a risk assessment to be conducted by the contractor to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of sensitive but unclassified information. While ****2**** performed a risk assessment for its overall environment, it did not conduct a risk assessment specifically of the ISAC. ****2*** thought they had met this requirement through the overall environment risk assessment; however, the CSA team informed ****2*** that a separate risk assessment is needed for the ISAC. ****2**** indicated it was in the process of developing a separate risk assessment for the ISAC, expecting to complete it by July 2017.

The lack of a risk assessment of the ISAC environment may result in risks not being properly assessed and raises the risk that vulnerabilities would persist and not be timely corrected or mitigated.

Flaw Remediation Policy was incomplete and not fully implemented

Publication 4812 requires contractors to identify, report, and correct information system flaws. Publication 4812 states that flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must be addressed expeditiously.

****2** developed the ISAC Flaw Remediation Policy and Procedures that included their policy for applying security patches. The policy specified that vulnerabilities of critical impact must be addressed immediately, those of medium impact must be addressed within 10 business days, and those of low impact must be addressed on a quarterly basis. However, we found some improvements were needed in the policy and its implementation.

- Policy did not specify the time frame for addressing high vulnerabilities. Although the policy specified time frames for addressing critical, medium, and low impact vulnerabilities, it did not specify a time frame to address vulnerabilities identified as high impact. ****2*** indicated that it would update its policy to set the time frame for addressing high-impact vulnerabilities to be within two weeks and remaining vulnerabilities (*i.e.*, medium and low) within 30 days.
- Vulnerabilities were not corrected timely. We reviewed vulnerability scanning reports for up to 16 ISAC servers for the period January 16, 2017, through June 5, 2017, that identified 35 critical, 114 high, and 447 medium vulnerabilities. ***2*** generally corrected its critical and high-impact vulnerabilities within reasonable time frames. We noted one exception: one ISAC server, in operation in January 2017, was not updated until March 2017 with a security patch that was released by the vendor in November 2016. This left the server exposed to high-level vulnerabilities, including **********2**********. ***2*** did not always correct medium vulnerabilities within its established time frame of 10 business days. Examples of medium vulnerabilities that persisted for 69 business days or longer included *****2*** **********2********** **********2**********.

  2 indicated that vulnerabilities were not always corrected timely because it had been in the process of changing its scan parameters while adding new personnel and upgrading system infrastructure. ***2*** indicated that it has resumed its normal practices of resolving vulnerabilities. However, scans that ***2***ran in June 2017 indicated that medium vulnerabilities involving the **********2********** still persisted on seven of the 16 ISAC servers.

When information system flaws are not timely corrected, vulnerabilities may be exploited.

POA&M processes needed improvement to ensure effective monitoring of weaknesses

Publication 4812 requires contractors to manage corrective actions for control failures identified during contractor security reviews in a POA&M and to provide POA&Ms quarterly to the IRS to demonstrate progress in correcting the weaknesses.

The IRS requires that POA&Ms comply with Office of Management and Budget standards that require specific items to be included, such as date found, due date, revised due date (if the POA&M exceeds its due date), status, actual completion date (when closing), due date comments, status comments, milestone status, and milestone due date.

2 prepared POA&Ms for the 33 information technology findings resulting from the IRS CSA review of the ISAC during the week of December 13, 2016. Subsequently, ***2*** has made significant progress in correcting the weaknesses identified during the CSA review. We

evaluated ***2*** POA&M tracking reports for the weeks of February 8, 2017, and April 13, 2017, which indicated that corrective actions were completed for 23 POA&Ms.

However, processes could be improved to ensure that POA&M weaknesses are adequately tracked and timely corrected. For example, we noted instances in which POA&M tracking reports were inconsistent in regards to tracking POA&Ms to completion and containing the data elements required by the IRS and the Office of Management and Budget.

- POA&Ms were missing. Two POA&Ms that were tracked on the February 2017 report were missing from the April 2017 report with no explanation for why they dropped off.
    - One POA&M was related to the ISAC System Security Plan. ***2*** indicated that the ISAC System Security Plan had been completed, so the POA&M was removed from the report. However, not documenting its completion caused confusion in regards to its status.
    - The second POA&M pertained to ensuring that proper reporting requirements were included in the Privacy Incident Response Plan. ***2*** indicated that the April 2017 POA&M report was subsequently corrected to include the missing POA&M regarding the Privacy Incident Response Plan that was still open.
- Data elements were missing. The February 2017 POA&M tracking report included status comments for tracking the progress being made, but the April 2017 POA&M tracking report did not. Neither report contained the data elements "milestone due date" or "actual completion date," nor were there revised due dates for POA&Ms when the status had passed the due date.

2 prepared the POA&Ms to address the CSA team's findings following its initial assessment in December 2016; however, they did not maintain consistency in the subsequent POA&M report. Tracking remediation of identified weaknesses is less effective when POA&Ms are inaccurate or incomplete and do not include necessary details to determine the proper status of corrective actions.

The physical security portion of the Computer Security Assessment has not been performed

Publication 4812 also states that the IRS Agency-Wide Shared Services' Facilities Management and Security Services (FMSS) office must collaborate with the CSA office to conduct the physical security portion of the CSA. Physical security controls include controls such as monitoring physical access and environment protection controls. However, the FMSS office has not yet performed the physical security portion of the CSA. FMSS officials indicated a physical security review was not conducted because they did not have any physical security specialists available during the time of the initial CSA. Without an assessment of the physical security controls at the ***2*** site, the IRS has no information on the status of these controls. The FMSS office scheduled the physical security portion of the review to be conducted during the

week of July 10, 2017; which is the same time the CSA team scheduled its follow-up review of the security controls, now that the ISAC is in operation.

Recommendations

Recommendation 1: The Director, Return Integrity and Compliance Services, should ensure that the ***2*** contractor fully implements required controls to include the ********2***** *********2*******, a privacy incident response plan, a risk assessment of the ISAC environment, and timely flaw remediation, and improves the POA&M process.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to actively monitor the contractor's progress pursuant to IRS Publication 4812. Although the ISAC does not possess any Federal tax information, the IRS plans to continue ensuring that ****2*** fully implements required controls, including the **********2**********. The IRS stated that actions have been completed for the development of a privacy incident response plan, timely flaw remediation, performance of a risk assessment of the ISAC environment, and improvements to eliminate noted deficiencies in the POA&M process.

Recommendation 2: The Director, FMSS, should ensure that the physical security portion of the CSA is performed and ensure that physical security deficiencies are corrected in a timely manner.

> ***Management's Response:*** The IRS agreed with this recommendation. In July 2017, the physical security controls portion of the CSA was completed. Through contract monitoring, the IRS plans to assess any deficiencies noted in the report and address them with ***2*** to ensure that corrective actions are fully implemented.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS developed the Identity Theft Tax Refund Fraud ISAC (hereafter referred to as ISAC) in accordance with Federal security standards to ensure that sensitive fraud data are protected against unauthorized access. To accomplish our objective, we:

I. Determined whether the data being maintained in the ISAC includes taxpayer, sensitive but unclassified, or Personally Identifiable Information, and whether its collection is in accordance with Federal privacy regulations.

   A. Reviewed relevant Federal regulations related to privacy and sensitive data to identify requirements regarding its creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal.

   B. Determined whether the IRS had properly implemented privacy requirements as they related to the ISAC.

   C. Determined the type of data being collected and maintained in the ISAC.

   D. Consulted with ISAC personnel to determine plans for future data gathering and use and any related plans to upgrade controls as needed.

II. Determined whether the IRS has implemented adequate security and privacy controls to protect the data maintained in the ISAC.

   A. Reviewed relevant Federal regulations and security guidelines for developing a secure ISAC system.

   B. Obtained and evaluated evidence that supported whether adequate security and privacy controls to protect ISAC data had been implemented.

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: Internal Revenue Manual Section 10.8.1, *Information Technology Security, Policy, and Guidance*; IRS Publication 4812, *Contractor Security Controls*; and other IRS controls and procedures related to ensuring the privacy and security of sensitive data. We evaluated these controls by interviewing IRS

management and staff; reviewing relevant NIST, Office of Management and Budget, ISAO, and IRS documentation; and reviewing relevant supporting documentation.

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Esther Wilson, Lead Auditor
Bret Hunter, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Commissioner, Wage and Investment Division
Chief, Criminal Investigation
Chief, Agency-Wide Shared Services
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Director, Privacy, Governmental Liaison, and Disclosure
Director, Office of Audit Coordination

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

SEP 07 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed (Audit # 201720006)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate the acknowledgment of the IRS' achievements in standing up the Identity Theft and Tax Refund Fraud Information Sharing and Analysis Center (ISAC). The IRS chartered the ISAC in December 2016 and began pilot operations on January 23, 2017. It was developed to provide a secure platform, among the ISAC membership, for sharing data and related analyses on ever-evolving patterns of identity theft (IDT) and tax refund fraud, and to improve detection, prevention, and deterrence capabilities. The ISAC is a product of the IRS' Security Summit activities, which, in 2015 undertook a holistic review of the threat of IDT refund fraud across the lifecycle of a tax return, at both the federal and state levels. Tangible benefits of these endeavors include the improvement of our fraud detection filters and systems that have led to substantial reduction in the number of individuals reporting themselves as victims of IDT. Over the past two filing seasons, the number of self-reported victims has declined by two-thirds.

As of April 2017, the ISAC has 36 member organizations from state departments of revenue and the tax software and tax preparation industries. The two primary capabilities being piloted this year are: (1) sharing of tax ecosystem alerts and (2) analysis of leads generated by the tax software and tax preparation industry and other member data. Tax ecosystem alerts are akin to a neighborhood listserv[1] for the group membership. Members report and share information and observations on threats they encounter so that others can protect themselves against the same or similar actions. Past threats have included the compromising of taxpayers' personally identifiable information through breaches of employer wage and withholding information and

[1] An application that distributes messages to subscribers on an electronic mailing list.

through the theft of client data from tax professionals. Information has also been shared on new and emerging schemes, and from the monitoring of chatter on the dark web[2] about system vulnerabilities. The ISAC enables the members to use the alerts to identify suspicious returns in their own systems and stop the further processing of returns seeking fraudulent refunds.

Members use the second capability, the analytical function, by submitting data to the **********2**********
**********2**********. In preparation for the 2018 filing season, the ISAC plans to perform several evaluations that will help identify data with the greatest predictive capabilities. It is anticipated that with its increased membership and improved understanding of which data are most relevant to identifying and reducing fraud, the ISAC will realize a greater level of effectiveness in the next filing season.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
****
**********2**********
**********2**********
**********2**********.

As your report acknowledges, the IRS does not store Federal Tax Information (FTI) in the ISAC, **********2**********
**********2**********
**********2**********
**********2**********. We agree with your recommendations and have already taken action that partially addresses them.

Attached are our comments and proposed actions to your recommendations. 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

[2] The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

Attachment

Recommendations

RECOMMENDATION 1
The Director, Return Integrity and Compliance Services, should ensure that the ***2*** fully implements required controls to include the ******2********** *********2**********, a privacy incident response plan, a risk assessment of the ISAC environment, and timely flaw remediation, and improves the POA&M process.

CORRECTIVE ACTION
We agree with this recommendation and are actively monitoring the contractor's progress pursuant to IRS Publication 4812, Contractor Security Controls. Although the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) does not possess any Federal tax information, we will continue to ensure that the **2**** ***2**** fully implements required controls, including **********2********* **********2**********. We have determined actions have been completed for development of a privacy incident response plan and timely flaw remediation, performance of a risk assessment of the ISAC environment, and improvements have been made to eliminate noted deficiencies in the plan of action and milestone processes.

IMPLEMENTATION DATE
April 15, 2018

RESPONSIBLE OFFICIAL
Director, 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 control system.

RECOMMENDATION 2
The Chief, Agency-Wide Shared Services, should ensure that the physical security portion of the CSA is performed and ensure that physical security deficiencies are corrected in a timely manner.

CORRECTIVE ACTION
We agree with this recommendation and have already taken action to address it. On July 13, 2017, the physical security controls portion of the Contractor Security Assessment (CSA) was completed. Through our contract monitoring process, we will assess any deficiencies noted in the report and address them with the ***2****** ********2******** to ensure corrective actions are fully implemented.

IMPLEMENTATION DATE
CSA Physical Security Controls Assessment – Implemented

Correction of CSA-identified deficiencies – October 15, 2018

RESPONSIBLE OFFICIAL
CSA Physical Security Controls Assessment – Chief, Agency-Wide Shared Services

Correction of CSA-identified deficiencies – Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
CSA Physical Security Controls Assessment – N/A

Correction of CSA-identified deficiencies – We will monitor this corrective action as part of our internal management control system.