

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Access to and Safeguarding Federal Tax Information, Investigating Unauthorized Access, and Ongoing Audits on the Security of Taxpayer Data

August 14, 2024

Memorandum Number: 2024-20S-034

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.

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



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

August 14, 2024

MEMORANDUM FOR: CHIEF INFORMATION OFFICER

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Memorandum – Access to and Safeguarding Federal Tax Information, Investigating Unauthorized Access, and Ongoing Audits on the Security of Taxpayer Data (Review No.: 2023N11.CR08)

This memorandum presents the second in a series of two memorandums in response to the February 16, 2023, request from the Chairman of the House Committee on Ways and Means. The Treasury Inspector General for Tax Administration (TIGTA) provided briefings to the Chairman and Members of the Committee on the leak of confidential taxpayer information. The topics addressed in this memorandum include access to taxpayer information maintained by the Internal Revenue Service (IRS), investigating unauthorized access, systemic issues TIGTA has previously reported to the IRS and/or Congress, and recently issued reports and ongoing audits related to these issues.

If you have any questions, please contact me or Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Background

In February 2023, the Chairman of the House Committee on Ways and Means sent a letter to the Inspector General for the Treasury Inspector General for Tax Administration (TIGTA) that referenced a news media outlet that, in June 2021, revealed a “massive leak of confidential tax information that the IRS [Internal Revenue Service] is charged with keeping secure.” At the time, the news media outlet stated that it had “obtained a vast trove of IRS data on the tax returns of thousands of the nation’s wealthiest people, covering more than 15 years,” and subsequently published a series of articles focusing on numerous American taxpayers. In January 2024, a former IRS contractor was sentenced to five years in prison for disclosing thousands of tax returns without authorization. The contractor, according to the Justice Department, abused their position as a consultant at the IRS by disclosing thousands of Americans’ Federal tax returns and other private financial information to news organizations. In May 2024, legislation was introduced in the U.S. House of Representatives that aims to increase penalties for unauthorized disclosure of taxpayer information from \$5,000, or imprisonment of not more than five years to \$250,000, or imprisonment of not more than 10 years.

Following our receipt of the Chairman’s letter, TIGTA agreed to conduct an evaluation addressing how the IRS grants access to and safeguards Federal Tax Information (FTI) maintained on its various information technology systems (hereafter referred to as “sensitive systems”) and provide information on unauthorized access cases and the difficulty prosecuting the cases, the systemic issues previously reported, and TIGTA’s recently issued reports and ongoing audits on these issues.¹

FTI refers to a return and return information protected from unauthorized disclosure under Internal Revenue Code § 6103.² According to the Internal Revenue Code, return information includes, among other things, a taxpayer’s identity, the nature or amount of their income, deductions, exemptions, assets, liabilities, net worth, tax withheld, or tax payments under Title 26. Unauthorized access and disclosure of taxpayer information could undermine the taxpaying public’s trust in the Federal tax system to safeguard confidential tax information.

Objective

The overall objective of this review was to gather sufficient information to: 1) summarize who has access to taxpayer information maintained by the IRS, 2) provide data on unauthorized access cases worked by TIGTA, 3) outline systemic issues previously identified by TIGTA, and 4) provide an overview of ongoing or planned work in these areas.

¹ See Appendix II for a glossary of terms.

² 26 U.S.C. § 6103.

Results of Review

Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information

TIGTA’s Office of Inspections and Evaluations reported in February 2024 that users are granted access to sensitive systems via the Business Entitlement Access Request System (BEARS) application and that the process is the same for employees and contractors.³ We also found that the IRS is evaluating steps to improve its ability to safeguard data housed on its sensitive systems. These steps include identifying and recording user actions when accessing sensitive data and tracking authorized and unauthorized attempts to remove sensitive data from its systems. The following is a summary of the key findings from TIGTA’s Office of Inspections and Evaluations report.

Who has access to sensitive information

We reported that the primary users permitted access to sensitive systems are IRS employees, TIGTA employees, and contractors. Additionally, the report indicated that certain external users can also be granted access to sensitive systems. These external users include the Joint Committee on Taxation, the Joint Statistical Research program, the U.S. Department of the Treasury Office of Tax Analysis, and external law enforcement agencies.

How many individuals and organizations have access to sensitive information

We reported that as of July 13, 2023, 153,120 users, of which 13,321 are contractors, have or had access to an IRS information technology system. Further, 91,661 users, of which 5,068 are contractors, had authorization to access one or more of the 276 sensitive systems. Figure 1 provides a breakdown of how the IRS classifies these 91,661 users in BEARS as employees or contractors as well as by the users’ employment status as active, inactive, or separated.

Figure 1: Current and Prior Users With Access to Sensitive Systems

User Type	Active	Inactive	Separated	Total
Employee	86,290	26	277	86,593
Contractor	5,066	0	2	5,068
Total	91,356	26	279	91,661

Source: TIGTA analysis of BEARS user data as of July 13, 2023.

How is sensitive information accessed and for what purpose

We reported that according to the IRS’s internal guidelines, the IRS performs prescreening investigative steps such as completing a Federal Bureau of Investigation fingerprint check, credit check, IRS Automated Labor and Employee Relations Tracking System check, Federal tax compliance check, and U.S. Citizenship check for employees and contractors. Once an individual is onboarded as a new employee, the IRS then initiates the complete background investigation.

³ TIGTA, Report No. 2024-IE-R008, *Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information* (Feb. 2024).

In addition, internal guidelines note that when feasible, all background investigations shall be completed, and suitability decisions made within a new employee's first year of service. However, contractors, unlike IRS employees, generally must have a background investigation with a favorable determination prior to being approved access to a sensitive system.⁴ As of July 2023, TIGTA identified 19 (less than 1 percent) of the 5,068 contractors' most recent background determinations were not favorable, yet all 19 contractors had network and sensitive system access. The IRS disabled network access for eight of the 19 contractors, and the remaining 11 contractors received a favorable determination to support their access to IRS systems.

We also reported that procedures to systematically remove users who no longer require access to sensitive systems were not always working as intended. Our evaluation identified that not all user accesses are timely removed once they are separated from the IRS. Specifically, we identified that 279 (less than 1 percent) of the 91,661 users with sensitive system access were listed in BEARS as separated and continued to have access to one or more sensitive systems as of July 13, 2023.

In response to concerns raised in our Office of Inspections and Evaluations report, the IRS stated it already takes steps to remove access when a contractor is identified as not having a favorable background determination. The IRS also stated it has fully implemented automated removal of user network access for employees and contractors separated in the IRS personnel system. In addition, the IRS has an ongoing effort to improve processes for the identification and resolution of any separated user accounts that have not been timely purged.

How is sensitive system access gained and how is sensitive information safeguarded

We reported that for a user to gain access to a sensitive system, the user must be granted both:

- Network Access – The ability to log on to the IRS network.
- Sensitive System Access – The ability to log on to a specific sensitive system within the IRS network.

The process to gain access to a sensitive system differs from system to system. Sensitive systems have their own separate protocols for how users access the system. For example, accessing sensitive systems may be through an application or software installed on the user's computer, or using a web-based browser with the user required to either input a user login or complete multifactor authentication using a Personal Identity Verification card. Although management noted that for users to gain access to a sensitive system, they first need to be granted network access, we found that there were 1,566 IRS Criminal Investigation users who had no evidence of any network access in BEARS but had access to at least one sensitive system.

We also reported that the IRS has implemented processes and procedures to try and safeguard FTI. These processes include:

- **Establishment of a Data Loss Prevention Program** – The IRS's Data Loss Prevention System is an automated tool that monitors outgoing unencrypted employee e-mail (including attachments) and web traffic to attempt to identify the unencrypted sending of Personally Identifiable Information (PII).⁵

⁴ Contractors may be given interim system and network access prior to the completion of a background investigation.

⁵ TIGTA's Office of Audit is conducting an audit to evaluate the IRS's controls to prevent the exfiltration of sensitive taxpayer data. This report is scheduled to be issued in September 2024.

- **Periodic Recertifications** – Managers must periodically recertify that users have a continued need for access to a sensitive system. IRS internal guidelines note that these recertifications ensure that users retain access only to the systems they need to complete their jobs. Non-privileged access users must be periodically recertified after a specified period. Whereas privileged access users will be recertified more frequently due to their level of access. According to the IRS, recertification is a key control to protect IRS data and systems from threats and help maintain the security of IRS networks. IRS management stated that the recertification process is automated and monitored for compliance by the IRS Cybersecurity function.

Unauthorized Access Cases and the Difficulty Investigating and Prosecuting the Cases

The Internal Revenue Manual (IRM) states that since the inception of the Integrated Data Retrieval System in 1972, the IRS has worked continuously to prevent and detect unauthorized access, attempted access, and inspection of taxpayer records in all IRS internal and external computer systems.⁶ On August 5, 1997, the Taxpayer Browsing Protection Act was signed into law making willful unauthorized access or inspection of taxpayer records a crime.⁷ The law states that, “Upon conviction, penalties can include fines up to \$1,000 and/or up to one year in prison (together with the costs of prosecution), as well as termination of employment for Federal employees. This law also established the right of taxpayers to seek civil damages in Federal court.”

The IRS established the Unauthorized Access, Attempted Access, or Inspection of Taxpayer Records (UNAX) program to identify unauthorized access by employees to tax return data and PII in response to the Taxpayer Browsing Protection Act of 1997. According to the IRS, the UNAX program is designed to ensure that willful unauthorized access or inspection of taxpayer records is a crime punishable upon conviction by fines, imprisonment, and termination of employment. Taxpayer records include hard copies of returns and return information, as well as returns and return information maintained on a computer. To protect sensitive information from being jeopardized, TIGTA proactively identifies IRS employees who inappropriately access and/or disclose private taxpayer information. Sensitive data can consist of FTI or PII. The UNAX program identifies possible UNAX violations and classifies them as:

- Section 301 Unauthorized access of taxpayer information.⁸
- Section 305 Unauthorized disclosure of taxpayer information.⁹

Figure 2 is a summary of recent UNAX violation cases.

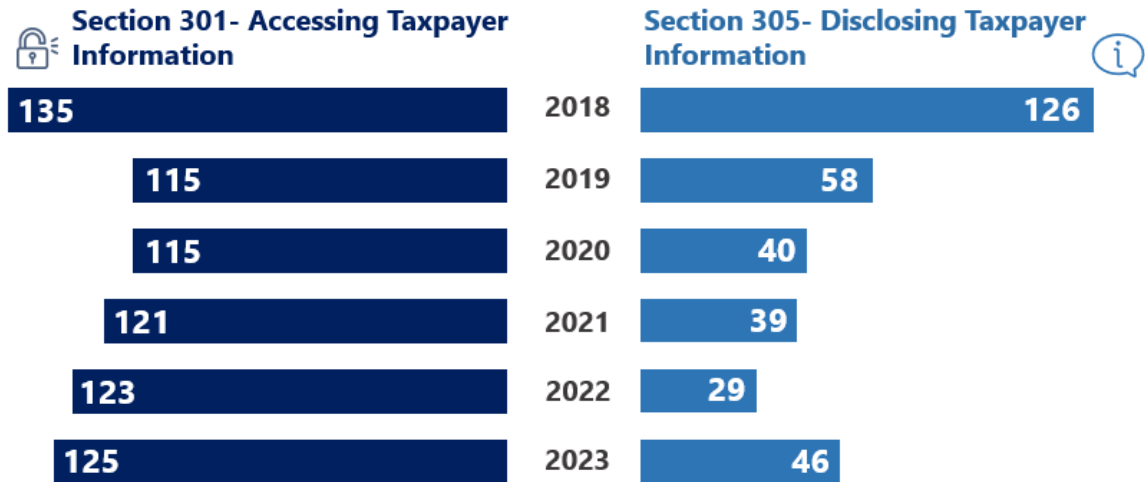
⁶ IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements* (Mar. 8, 2023).

⁷ 26 U.S.C. §§ 7213, 7213A, and 7431 (2018).

⁸ 26 U.S.C. § 7213A (1997).

⁹ 26 U.S.C. § 7213 (1997).

**Figure 2: Sections 301 and 305 UNAX Violation Cases
From Fiscal Years (FY) 2018 Through 2023 (as of July 13, 2023)**



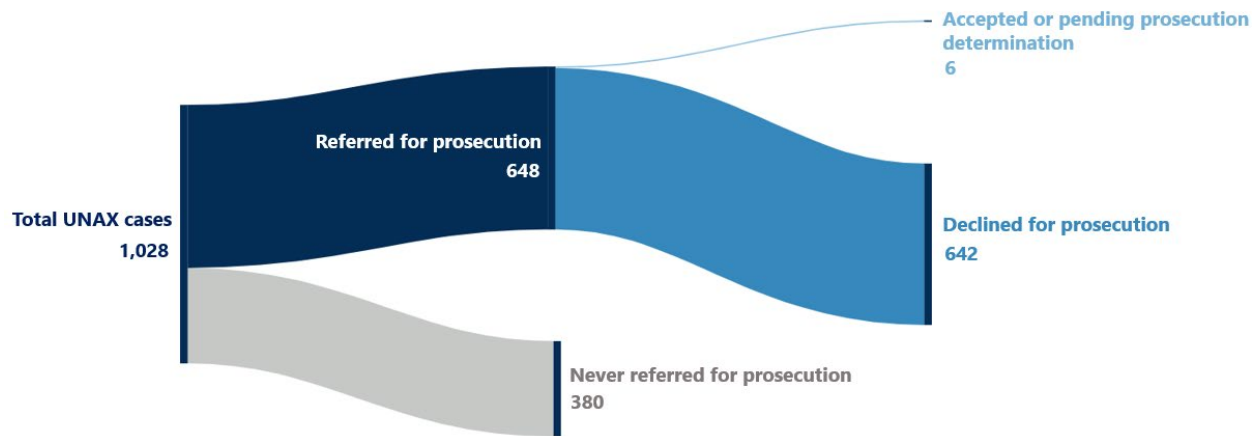
Source: TIGTA’s analysis of Sections 301 and 305 violations from FYs 2018 through 2023 (as of July 13, 2023). Note: The numbers within Figure 3 are distinct counts. There was a total of 1,028 UNAX violation cases investigated; however, because some cases have both Sections 301 and 305 violation codes, the Sections 301 and 305 columns cannot be added to get the total cases for the fiscal year.

From FYs 2018 through FY 2023 (as of July 13, 2023), there were a total of 1,028 UNAX violation cases investigated by TIGTA. As of July 13, 2023:

- 642 (62 percent) cases were referred but declined for prosecution.
- 380 (37 percent) cases were never referred for prosecution.
- 6 (less than 1 percent) cases have been accepted for prosecution or are pending prosecution determination.

Figure 3 illustrates the results of the 1,028 UNAX violation cases.

**Figure 3: Results of UNAX Violation Cases Investigated
by TIGTA From FY 2018 Through FY 2023 (as of July 13, 2023)**



Source: TIGTA’s analysis of Sections 301 and 305 violations from FYs 2018 through 2023 (as of July 13, 2023).

The reasons for the non-referral of a case for prosecution may include that the allegation was disproved, or the alleged unauthorized access was deemed inadvertent.

The decision on whether to prosecute an individual for violations is ultimately made by a prosecutor. TIGTA's Office of Investigations refers most of its cases to one of the approximately 93 U.S. Attorney's Offices in the United States and its territories. If the case involves additional tax-related violations, it may require referral to one of the three Department of Justice's Tax Divisions instead. Each of these offices uses its own criteria to determine if the violations substantiated by the investigation will be prosecuted by their office. TIGTA's Office of Investigations case management system tracks reasons for declination for most cases. Some common factors used by local U.S. Attorney's Offices to determine whether a violator will be prosecuted include the number of accesses made by the employee, the reason for the access, and whether the accessed information was subsequently disclosed.

In addition, while working on UNAX violation cases, TIGTA's Office of Investigations has encountered several challenges such as an individual moving protected data to a location where access cannot be regulated and tracked, technological limits to identifying sensitive data by the data structure alone, individualized encryption and storage scenarios restricting the access of investigators, and the use of personal or non-IRS e-mail to transmit sensitive information. These issues have been communicated to the IRS, and TIGTA's Office of Investigations has proposed solutions to the IRS to improve data security and its investigations. Some of the proposed solutions include:

- Establishing formal categorization of the sensitivity of IRS agency data.
- Limiting the ability to transfer data within the IRS.
- Implementing access-based audit logging for areas storing sensitive data.
- Disabling external storage of data.
- Using a master encryption key for authorized data storage.
- Providing refresher training on appropriate methods of data transfer to include the disclosure process.

We requested a response from the IRS as to which actions it had taken regarding these proposed solutions. The IRS responded on June 27, 2024, that the agency continues to modernize and enhance its data security protections and stated that the following steps have been taken to bolster the data protections proposed by TIGTA's Office of Investigations:¹⁰

- **Categorizing Sensitive IRS Data.** The Privacy, Governmental Liaison, and Disclosure organization is leading an enterprise-wide effort to implement sensitivity data labeling based on Controlled Unclassified Information Federal directives. Leveraging this categorization, the IRS has configured its software products to enable assignment of these sensitivity labels to improve controls for the storing and sharing of documents containing sensitive information. We plan to review this as part of our FY 2025 audit plan while evaluating the maturity of the IRS's data inventory management, categorization, availability, access, encryption, incidence response, and governance.
- **Limiting Internal Sharing of Sensitive Information.** The IRS stated it deploys robust processes to identify potential unauthorized accesses or inspection of tax information

¹⁰ These steps are statements from the IRS. TIGTA did not make any conclusions regarding the veracity of these statements.

and refers potential unauthorized accesses to TIGTA for formal investigation. To ensure that only those employees with a need to know are afforded access to sensitive information, the IRS has implemented enhanced enterprise identity and access management capabilities by deploying two systems recommended by the Department of Homeland Security. These systems ensure that access approvals for systems with sensitive information are approved by management, recertified routinely to ensure that continued access is warranted, and access roles are based on the principle of least privilege. We plan to review this as part of our FY 2025 audit plan when we evaluate the IRS's Enterprise Data Platform governance and management framework to determine its effectiveness in ensuring high data quality and accuracy, compliance with regulatory requirements and policies, and data security controls to protect sensitive information.

- **Improving Audit Logging.** The IRS stated it has completely modernized its Enterprise Security Audit Trails program to improve the capture of detailed auditing and logging information from IRS information systems, with a distinct focus on those information systems that process PII and FTI. The expanded Enterprise Security Audit Trails capability now provides consolidated audit data within a centralized repository and enhanced tools to manage and analyze internal and external attempts to access sensitive data and identify potential anomalous activity. We are planning a follow-up audit in FY 2025 to determine whether the IRS's Enterprise Security Audit Trails program was effectively implemented to meet Federal and IRS requirements.
- **Disabling External Storage of Data.** The IRS stated it has dramatically reduced users' ability to connect removable media, such as thumb drives and optical Compact Disc and Digital Versatile Disc to its computers. Further, it also stated it has disabled the use of external storage devices and implemented a new protocol that requires executive approval for users with legitimate business needs. These steps have significantly curtailed opportunities to remove sensitive taxpayer information from the IRS computing environment. The IRS also strengthened e-mail controls involving taxpayer information, including new restrictions on the ability to e-mail information outside the IRS, while preserving but closely monitoring this ability when necessary for collaborating with non-IRS employees.
- **Enhancing Encryption Methods.** The IRS stated it has implemented encryption for data in transit and data at rest as part of its Federal Information Security Modernization Act of 2014 improvement goals.¹¹
- **Enhancing Awareness of Data Protection Responsibilities.** The IRS stated that in 2023, it provided a full suite of training courses for all security specialties and knowledge levels to ensure full compliance with mandatory contractor security training. For contractors, the IRS stated it implemented a zero-tolerance policy for noncompliance with security training by automatically deprovisioning their network access when their training has not been completed. Further, the IRS stated in 2024 that it has issued numerous reminders to the IRS workforce to reiterate the criticality of protecting sensitive data, the process to request access to sensitive data, the formal process to report any inadvertent access not supported by case assignments, and the potential penalties of monetary fines and imprisonment for willful unauthorized accesses.

¹¹ Pub. L. No. 113-283.

Management and Performance Challenges Facing the IRS

The Reports Consolidation Act of 2000 requires that TIGTA summarize, for inclusion in the annual *Department of the Treasury Agency Financial Report*, its perspective on the most serious management and performance challenges confronting the IRS.¹² Each year, TIGTA evaluates IRS programs, operations, and management functions to identify the areas of highest vulnerabilities to the Nation's tax system. TIGTA has consistently listed security over taxpayer data as a management and performance challenge for more than 10 years. The narrative supporting the assessment of the challenge provided observations and results of reviews regarding the security over taxpayer data. For example, in FY 2014, TIGTA commented that computer security has been problematic for the IRS since 1997, when the IRS initially reported computer security as a material weakness during its annual evaluation of internal accounting and administrative controls. The IRS did not implement some of the additional countermeasures that were identified by the completed risk assessments.

In our FY 2015 major management challenges memorandum, TIGTA highlighted our report that found that eight (42 percent) of the 19 Planned Corrective Actions (PCA) had not been fully implemented and should not have been closed.¹³ These PCAs involved systems containing taxpayer data. In FY 2016, TIGTA commented that cybersecurity threats against the Federal Government continue to grow. For example, in May 2015, the IRS announced that criminals had used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to tax account information through the IRS's Get Transcript application.¹⁴ TIGTA also found that many interconnections in use at the IRS do not have proper authorization or security agreements.

In FY 2018, TIGTA commented that its Office of Investigations' data analysis techniques have identified IRS employees who access taxpayer records without authorization and then use the information to engage in illegal activities. We also expressed concerns about the IRS's logging and monitoring capabilities over all connections to IRS online services. In FY 2020, TIGTA commented that in addition to external threats, the IRS must ensure that its systems and data are protected against internal threats. For example, in February 2019, an IRS employee was indicted for the unauthorized disclosure of Suspicious Activity Reports, misuse of a Government computer, and misuse of a Social Security Number in violation of the law.¹⁵ In our FY 2021 major management challenges memorandum, we discussed our report which found that the IRS continues to struggle with ensuring that all applications are providing complete and accurate audit trails for monitoring and identifying unauthorized access.¹⁶ TIGTA also found that the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and PII.

In our FY 2022 major management challenges memorandum, TIGTA highlighted our report that found that the IRS continues to digitize many of the previously paper processes, which generates targets of opportunity for malicious actors around the globe. Also, TIGTA remarked that the IRS decided to leverage the Security Summit to disclose return information related to

¹² 31 U.S.C. § 3516(d) (2006).

¹³ TIGTA, Report No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).

¹⁴ Information available on the Get Transcript application can include account transactions, line-by-line tax return information, and income reported to the IRS.

¹⁵ *U.S. v. Fry*, Case No. 3:19-CR-00102-EMC (N.D. CAL 2019), Sentencing Memorandum.

¹⁶ TIGTA, Report No. 2020-20-033, *Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information* (July 2020).

refund fraud schemes to State tax agencies and industry partners. However, we reported that additional policies, procedures, and actions are needed to improve the effectiveness of security over the sharing and storing of the data.¹⁷

In FY 2023, TIGTA highlighted that the IRS initially required taxpayers to use a third-party service, ID.me, to help authenticate individuals creating online accounts by using facial recognition to verify their identity for the 2022 Filing Season. However, in response to privacy concerns related to taxpayers providing biometric data to a private company, the IRS announced in February 2022 that taxpayers could sign up for IRS online accounts with ID.me without the use of any biometric data.

Systemic Issues Previously Reported to the IRS and/or Congress

The IRS Cybersecurity function analyzes system security reports obtained from the centralized data repository that collects audit logs from various applications. Audit logs are a chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to results. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Recent cybersecurity events underscore the importance of increased visibility before, during, and after a cybersecurity incident. Audit logs provide both TIGTA and the IRS information necessary to detect unauthorized access to IRS systems and data to reconstruct events for potential criminal investigations.

TIGTA reports with audit trail-related recommendations and corrective actions

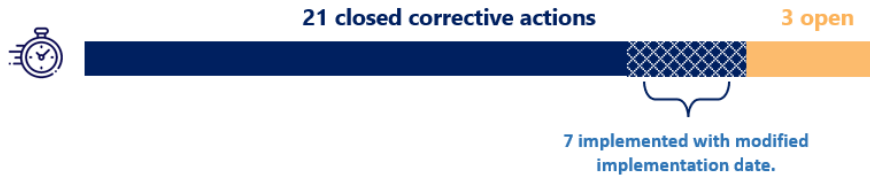
We identified and reviewed 13 TIGTA reports with findings related to audit trails during FYs 2018 through 2023. Based on our analysis, we identified 24 recommendations with 21 closed corrective actions and three open corrective actions.¹⁸ The three open corrective actions are due to be completed in FYs 2024 and 2025. Figure 4 provides a summary of the IRS corrective action status for TIGTA audit trail-related findings.

¹⁷ TIGTA, Report No. 2021-25-025, *Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center* (May 2021).

¹⁸ Appendix I provides a summary of the TIGTA audit trail-related findings with the recommendations, proposed implementation dates, and status of IRS corrective actions.

Figure 4: Summary of IRS Corrective Action Status for TIGTA Audit Trail-Related Findings Reported in FYs 2018 Through 2023

In response to TIGTA issued reports between FYs 2018 through 2023, the IRS modified the implementation date for **33 percent** of closed corrective actions.



Source: TIGTA analysis of our FYs 2018 through 2023 audit trail-related findings.

We reviewed the Joint Audit Management Enterprise System (JAMES) reports for 24 recommendations, corrective action implementation dates, and statuses. We found that the IRS Program Office had modified the implementation due dates for seven (33 percent) of the 21 closed corrective actions.

Significant audit trail-related findings from prior TIGTA reports

As previously stated, the IRS is responsible for protecting taxpayer information maintained on its various information technology systems. Audit logs provide both TIGTA and the IRS information necessary to detect unauthorized access to IRS systems and data to reconstruct events for potential criminal investigations. The following is a summary of some significant audit trail-related findings from TIGTA reports.

- TIGTA, Report No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018). We found that the IRS did not fully implement the PCAs on closed TIGTA cybersecurity recommendations. Specifically, TIGTA reviewed a judgmental sample of 23 closed PCAs and found the IRS fully implemented 13 PCAs. Consequently, one PCA was not implemented and nine PCAs were only partially implemented.
- TIGTA, Report No. 2020-20-033, *Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information* (July 2020). We found that implemented audit trail solutions were not effective, and the IRS continues to have challenges with ensuring that all applications are providing complete and accurate audit trails for monitoring and identifying unauthorized access and for other investigative purposes. Specifically, the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and PII. This inventory is critical as a baseline for all applications that need to be monitored for potential unauthorized access by employees. In addition, not all applications with audit trail deficiencies were being tracked and monitored as required, which could allow unresolved deficiencies to persist indefinitely.
- TIGTA, Report No. 2022-20-052, *Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk* (Sept. 2022).

. Encryption is a key control for protecting the taxpayer data on IRS

cloud services. [REDACTED]

- TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (Oct. 2023). We found that the Department of the Treasury reported that the IRS was at Event Logging maturity level two for the Federal Information Security Modernization Act of 2014 reportable systems as of May 2023.¹⁹ We could not conclude whether the IRS currently meets all Event Logging requirements because the IRS has not documented and demonstrated compliance of all systems with Office of Management and Budget requirements.

Also, the IRS determined that 356 systems have application logging requirements. As of June 2023, 231 (65 percent) systems were sending event logs to the data repository, but 125 (35 percent) systems were not sending event log data to its data repository. In response to our draft report, the IRS stated that 37 of the 356 previously identified systems did not require application logging. For the remaining 319 systems, the IRS further stated that by September 30, 2023, it completed implementing logging requirements on 318 of 319 systems and temporarily removed the remaining legacy system. In addition, the IRS is not effectively identifying and tracking all systems and applications to ensure that audit trail data are collected in the data repository.

Finally, the IRS is not properly managing user accounts for its data repository. Specifically, we reviewed authorized users for two system modules containing audit trail information and found that 18 users previously approved by their manager did not have a business justification for retaining the access. As of June 2023, each of the 18 users without a valid business justification had their access to the two modules removed.

Recently Issued Reports and Ongoing Audits on the Security of Taxpayer Data

Recently issued reports

Privacy program controls

In June 2023, we reported that our review of a 2022 year-end privacy awareness training compliance report of IRS contractors found that 3,881 (21 percent) of 18,688 contractors have not taken the required annual privacy awareness training.²⁰ Specifically, 2,365 contractors with network access and 1,516 contractors without network access did not take the privacy awareness training. Before any contractor employee is given access to taxpayer records, including returns maintained on an information system, they shall have been approved for staff-like access and certify they have been provided unauthorized access training. Without completing the required training, IRS contractors are at increased risk of being unprepared to handle taxpayer information.

¹⁹ 44 U.S.C. §§ 3551-3558.

²⁰ TIGTA, Report No. 2023-20-034, *Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed* (June 2023).

Form 990-T, Exempt Organization Business Income Tax Return, data leak

According to the IRS, on August 8, 2022, the IRS's Research, Applied Analytics, and Statistics (RAAS) organization discovered that Forms 990-T data from non-501(c)(3) charities were inappropriately posted to the Tax Exempt Organization Search web page beginning in February 2021.²¹ The IRS took immediate action to remove the files and diagnose the problem. The Department of the Treasury notified Congress on September 2, 2022, via a seven-day letter as required. The IRS also notified the Department of the Treasury's Security Operations Center and TIGTA of the disclosure and posted public notice of the disclosure on IRS.gov.

In November 2022, a second inadvertent disclosure incident occurred when the IRS was reposting information that had been temporarily removed from the Tax Exempt Organization Search web page while implementing preventative measures. On November 29, 2022, the IRS contractor began the process of posting files. On December 1, 2022, an external party notified the IRS that the newly released files that were posted by the contractor appeared to be a subset of the files from the first unauthorized disclosure. According to IRS management, they immediately asked the contractor to remove the data from the Tax Exempt Organization Search web page. The Department of the Treasury reported to Congress in a seven-day letter dated December 15, 2022, that the error occurred because the old files had not been purged by the contractor.

In September 2023, we performed a review to evaluate the effectiveness of the IRS's actions to address the control weaknesses resulting in the inappropriate disclosure of Form 990-T data.²² We concluded that the IRS is establishing new processes to prevent future unauthorized disclosure of Form 990-T. The IRS implemented a new posting process and modified its contract to ensure that Form 990-T data are not stored in contractor-owned storage and are timely deleted by the contractor. The IRS also implemented a two-part quality control process. The quality control process involves statistical sampling of Forms 990-T and a review process to verify the returns files are disclosable.

Ongoing audits

Disclosure of FTI to State agencies

In FY 2023, TIGTA's Office of Audit began reviewing the disclosure of returns and return information to State agencies. The objective of this audit is to determine if the Office of Safeguards provides adequate oversight of State agencies receiving FTI.²³ As a condition of receiving FTI, the receiving agency must show the ability to protect the confidentiality of that information. Internal Revenue Code § 6103(p)(4)(E) requires agencies to file a Safeguard Security Report that describes the procedures established and used by the agency for ensuring the confidentiality of information received from the IRS. This audit will determine if the Office of Safeguards receives and reviews Safeguard Security Reports for State agencies requesting access to FTI. This audit has an estimated completion date of August 2024.

In addition, TIGTA plans to perform a series of Information Sharing Arrangement reviews starting with the disclosure of FTI to State agencies, and each review will cover a different

²¹ In compliance with the Taxpayer First Act [Pub. L. No. 116-25, 133 Stat. 981 (2019) (codified in scattered sections of 26 U.S.C.)] and a court order, beginning in 2021, the IRS began posting files to the Tax Exempt Organization Search page in a machine-readable (XML) format rather than in a Portable Document Format (PDF).

²² TIGTA, Report No. 2023-2S-069, *The IRS Implemented Processes to Prevent Future Unauthorized Disclosures of Form 990-T Information* (Sept. 2023).

²³ TIGTA, Audit No. 202310007, *Disclosure of Federal Tax Information to State Agencies*.

segment of FTI recipients. IRS information sharing programs save government resources through partnerships between IRS and Federal, State, and municipal governments. These programs include the exchange of taxpayer data with the goal of enhancing voluntary compliance with tax laws.

Contractor employee separations and transfer procedures

In FY 2023, TIGTA's Office of Audit began a review to assess the effectiveness of controls over select contractor employee processes, including the removal of contractor access to IRS facilities, systems, and equipment upon separation.²⁴ Contractors with staff-like access affords them unescorted access to IRS-owned and -controlled facilities, information systems, and sensitive but unclassified information. An objective of this audit is to determine if the IRS performs revalidation of contractor employees with staff-like access in case of material change in the working status of the contractor employee. This audit has an estimated completion date of September 2024.

RAAS data security

In FY 2023, TIGTA's Office of Audit began a review of the RAAS Compliance Data Warehouse (CDW) Security.²⁵ The overall objective of this audit is to determine whether sufficient security safeguards over the CDW exist to protect taxpayer data against unauthorized access. The CDW is not a traditional computer software application. At its core, the CDW is a massive data warehouse containing multiple years of tax data consolidated from multiple sources, internal and external to the IRS. The primary goal of the CDW is to provide a single, integrated environment of data computing services to support the research and analysis needs of IRS employees. In addition, a secondary objective of the audit is to determine if the CDW is included as part of the IRS's User Behavior Analytics Capability system inventory and assess the effectiveness of managing potential insider threats. This audit has an estimated completion date of August 2024.

Controls over the exfiltration of taxpayer data

In FY 2023, TIGTA's Office of Audit began a review of the IRS's Controls Over the Exfiltration of Taxpayer Data.²⁶ The overall objective of this audit is to evaluate the IRS's controls to prevent the exfiltration of sensitive taxpayer data. Data exfiltration is typically caused by an outsider attack, careless inadvertent insider threat, or in some cases malicious insider threat. The IRS started the implementation of the Safeguarding Personally Identifiable Information Data Extracts Data Loss Prevention software solution in Calendar Year 2010. The IRS is entrusted with protecting information received from taxpayers and allowing this information to be removed or exfiltrated for unauthorized purposes could erode public trust. This audit has an estimated completion date of September 2024.

²⁴ TIGTA, Audit No. 202310026, *Contractor Separation and Transfer Procedures*.

²⁵ TIGTA, Audit No. 202320017, *Research, Applied Analytics, and Statistics Compliance Data Warehouse Data Security*.

²⁶ TIGTA, Audit No. 202320025, *Controls Over the Exfiltration of Taxpayer Data*.

Conclusion

The protection of FTI and PII has been a long-term challenge for the IRS, and while the IRS continues to make improvements to its controls over the security and privacy of taxpayer data, additional actions are needed. TIGTA will continue our oversight efforts in this critically important area.

Performance of This Review

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Federal Offices of Inspector General*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented.

Major contributors to the review were Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Daniel Preko, Audit Manager; and Suzanne Westcott, Lead Auditor.

TIGTA's Audit Trail-Related Recommendations and IRS Corrective Action Implementation Dates and Statuses

February 5, 2018

Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented

Report Number 2018-20-007

Recommendation 3: The Chief Information Officer should ensure that Electronic Authentication audit log captures [REDACTED] in a separate field for all user transactions to allow for tracking and analysis of user activity.

IRS Response: The IRS agreed with this recommendation. Information Technology staff will modify the reauthentication audit log process to capture [REDACTED] in a separate field for all user transactions. This modification will be assessed and prioritized along with all other Electronic Authentication work in the product backlog.

PCA Implementation Due Date: April 15, 2018

Modified Due Date: September 15, 2019

PCA Status: Closed on August 19, 2019

Recommendation 4: The Chief Information Officer should ensure that IRS policy is met in regards to audit log report generation and review, that actionable events and threshold triggers are kept current, and reports are useful for investigation and response to suspicious activities.

IRS Response: The IRS agreed with this recommendation. Cybersecurity staff will continue to implement the capability to generate reports from the Electronic Authentication audit logs, which enables on-demand audit review, analysis, and after-the-fact investigations. Additionally, Cybersecurity staff will continue to implement process changes to ensure that actionable events, threshold triggers, and reports are kept current.

PCA Implementation Due Date: October 15, 2018

PCA Status: Closed on October 15, 2018

February 7, 2018

Actions Are Needed to Reduce the Risk of Fraudulent Use of Employer Identification Numbers and to Improve the Effectiveness of the Application Process

Report Number 2018-40-013

Recommendation 11: The Commissioner, Wage and Investment Division, should establish systemic processes for the Modernized Employer Identification Numbers to alert system administrators when error code counts reach certain thresholds based on historical trends.

IRS Response: The IRS agreed with this recommendation. IRS management plans to seek a feasible process for the Modernized Employer Identification Number to alert

system administrators when error code counts reach certain thresholds based on historical trends.

PCA Implementation Due Date: October 15, 2018

Modified Due Date: April 15, 2019

PCA Status: Closed on March 14, 2019

Recommendation 12: The Commissioner, Wage and Investment Division, should revise procedures to not allow applicants to designate another business as the responsible party.

IRS Response: The IRS agreed with this recommendation. IRS management stated they are currently assessing a proposed policy change to determine the impact to other processes before moving forward with implementation activities.

PCA Implementation Due Date: December 15, 2018

Modified Due Date: June 15, 2019

PCA Status: Closed on June 7, 2019

June 21, 2018

The Cybersecurity Data Warehouse Needs Improved Security Controls

Report Number 2018-20-030

Recommendation 3: The Chief Information Officer should ensure that automated controls and processes to capture and monitor the activities of all IRS personnel with access to transactional audit logs containing taxpayer data in the Cybersecurity Data Warehouse are implemented.

IRS Response: The IRS agreed with this recommendation. During the audit, the Cybersecurity organization implemented enhanced auditing controls for the Cybersecurity Data Warehouse to capture the activities performed by analysts and administrators. Efforts are underway to ensure ongoing monitoring of transactions by analysts and administrators.

PCA Implementation Due Date: March 15, 2019

Modified Due Date: August 15, 2019

PCA Status: Closed on August 1, 2019

September 19, 2018

Improved Controls Are Needed to Ensure That Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure

Report Number 2018-20-063

Recommendation 2: The Chief Financial Officer should ensure that sufficient supporting documentation is uploaded to the JAMES to support PCA closure.

IRS Response: The IRS agreed with this recommendation. The Office of Audit Coordination will continue to conduct reviews throughout the year of a sample of closed PCAs to ensure that the IRS meets documentation requirements. As the IRS updates the Audit Coordination IRM and guidance, it will evaluate the existing review criteria to determine if the criteria needs to be improved.

PCA Implementation Due Date: May 15, 2019

Modified Due Date: March 15, 2021

PCA Status: Closed on February 5, 2021

September 20, 2018

Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented

Report Number 2018-20-066

Recommendation 1: The Chief Information Officer should change the PCA status from closed to open in the JAMES for the corrective actions TIGTA identified as not fully implemented and the status of the PCAs should remain open until they are fully implemented.

IRS Response: The IRS agreed with this recommendation. The Cybersecurity organization will work with the Office of Strategy and Planning to reopen the PCAs TIGTA identified as not fully implemented. The PCAs will remain open in the JAMES until they are fully implemented.

PCA Implementation Due Date: March 15, 2019

Modified Due Date: August 15, 2019

PCA Status: Closed on August 15, 2019

September 12, 2019

E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive

Report Number 2019-20-060

Recommendation 2: The Chief Information Officer should ensure that the appropriate Enterprise Life Cycle criteria and methodology are consistently applied.

IRS Response: The IRS agreed with the recommendation. The IRS will update IRM 2.16.1 to provide guidance and criteria for infrastructure projects to ensure consistency across the Information Technology organization.

PCA Implementation Due Date: September 15, 2020

PCA Status: Closed on September 9, 2020

February 5, 2020

Active Directory Oversight Needs Improvement

Report Number 2020-20-006

Recommendation 8: The Chief Information Officer should review all business role accounts in the Integrated Submission and Remittance Processing Active Directory forests and ensure that they are in compliance with IRM policy regarding account disabling, quarantining, and removal.

IRS Response: The IRS agreed with this recommendation. The Chief Information Officer will review all business role accounts in the Integrated Submission and Remittance Processing Active Directory forests and ensure that they are following IRM policy regarding account disabling, quarantining, and removal.

PCA Implementation Due Date: December 15, 2020

PCA Status: Closed on November 5, 2020

June 1, 2020

Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented

Report Number 2020-20-022

Recommendation 4: The Chief Risk Officer should ensure that any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally sampled PCAs that lacked sufficient documentation to support their closure.

IRS Response: The IRS agreed with this recommendation. The Chief Risk Officer has begun to put in place procedures to ensure that any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally scripted PCAs that lacked sufficient documentation to support the closure.

PCA Implementation Due Date: June 15, 2021

PCA Status: Closed on June 15, 2021

July 31, 2020

Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information

Report Number 2020-20-033

Recommendation 1: The Chief Information Officer should ensure that the Cybersecurity function; the Privacy, Governmental Liaison, and Disclosure office; and application owners develop and implement a methodology to identify and annually update the inventory of all applications that store or process taxpayer data and PII for the purpose of detecting improper cyber activities and to reconstruct events for potential criminal investigations. Furthermore, audit trail records for the applications should be included in the Security Audit and Analysis System.

IRS Response: The IRS partially agreed with this recommendation. The Cybersecurity function will partner with the Privacy, Governmental Liaison, and Disclosure office to review and revise the current Privacy Impact Management System to clearly identify applications that store, process, or transact FTI for the purpose of detecting improper cyber activities and to reconstruct events for potential criminal investigations. This inventory will be updated, at a minimum, annually. The IRS will be replacing the Security Audit and Analysis System; however, audit trails records will continue to be tracked in a centralized system.

PCA Implementation Due Date: September 15, 2021

PCA Status: Closed on July 30, 2021

Recommendation 2: The Chief Information Officer should obtain the list of 13 applications with an Audit Control Response that references the obsolete IRM, conduct a revalidation of the auditable events, and issue an Audit Trail Deficiency Memorandum to the application owner, if needed, to require an Audit Control

Response update to comply with the current list of auditable events. In addition, ensure that revalidations are conducted annually as required.

IRS Response: The IRS agreed with this recommendation. The Cybersecurity function will obtain the list of 13 applications with the Audit Control Responses that reference the obsolete IRM, correct the reference to reflect current policy, conduct revalidations against the current list of auditable events, and issue Audit Trail Deficiency Memorandums to application owners. If changes to the audit trails are identified, an Audit Control Response revalidation is conducted annually, as required.

PCA Implementation Due Date: [October 15, 2021](#)

PCA Status: [Closed on September 15, 2021](#)

Recommendation 3: The Chief Information Officer should ensure that application audit trail deficiencies are properly tracked on a Plan of Action and Milestones, thus ensuring compliance with the Federal Information Security Modernization Act of 2014, IRM policy, and the Office of Management and Budget annual guidance.

IRS Response: The IRS agreed with this recommendation. The Cybersecurity function will ensure that currently identified application audit trail deficiencies are properly tracked in a Plan of Action and Milestones in accordance with the Federal Information Security Modernization Act of 2014, IRM policy, and the Office of Management and Budget annual guidance.

PCA Implementation Due Date: [February 15, 2021](#)

PCA Status: [Closed on January 28, 2021](#)

Recommendation 4: The Chief Information Officer should ensure that IRM policy and the Audit Trail Deficiency Memorandum template document clearly and consistently communicate each stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the Plan of Action and Milestones is reflective of the issues indicated in the Audit Trail Deficiency Memorandum within 60 calendar days.

IRS Response: The IRS agreed with this recommendation. The policy is in place and compliant with National Institute of Standards and Technology and Department of the Treasury audit trail controls. The Audit Trail Deficiency Memorandum template will be revised to clearly and consistently communicate stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the Plan of Action and Milestones is reflective of the issues indicated in the Audit Trail Deficiency Memorandum within 60 calendar days.

PCA Implementation Due Date: [February 15, 2021](#)

PCA Status: [Closed on November 18, 2020](#)

Recommendation 5: The Chief Information Officer should establish a process improvement, so application owners timely create the Plan of Action and Milestones when audit trail deficiencies are identified. This recommendation also addresses a similar repeat finding from the FY 2015 audit report previously mentioned.¹

¹ TIGTA, Report. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015).

IRS Response: The IRS agreed with this recommendation. The Cybersecurity function will document within the Plan of Action and Milestones Standard Operating Procedures process improvements to require that application owners create the Plan of Action and Milestones timely when audit trail deficiencies are identified.

PCA Implementation Due Date: February 15, 2021

PCA Status: Closed on September 30, 2020

June 3, 2021

Improvements Are Needed to More [REDACTED] the Virtual Host Infrastructure Platform

Report Number 2021-20-024

Recommendation 5: The Chief Information Officer [REDACTED]
[REDACTED]
[REDACTED].

IRS Response: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

PCA Implementation Due Date: June 15, 2022

PCA Status: Closed on June 2, 2022

September 21, 2022

Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened

Report Number 2022-20-051

Recommendation 6: The Chief Information Officer should ensure that the Counter Insider Threat Operations branch starts reviewing the audit trails for the Taxpayer Digital Communications platform.

IRS Response: The IRS agreed with this recommendation. The Annual Security Control Assessment for eGain (Taxpayer Digital Communications Platform commercial implementation) was completed on May 4, 2022, and identified that the audit trail capture was not functioning as required. The IRS remediated the issue, and the audit log capture resumed prior to the end of May 2022. The Counter Insider Threat Operations branch will continuously monitor eGain audit trails per IRM guidelines.

PCA Implementation Due Date: February 15, 2023

PCA Status: Closed on February 15, 2023

September 27, 2022

Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk

Report Number 2022-20-052

Recommendation 1: The Chief Information Officer should expedite full implementation of the cloud security control infrastructure, *****2*****
*****2*****.

IRS Response: The IRS partially agreed with this recommendation. The IRS has a robust and comprehensive security control infrastructure documented within IRMs 10.8.1 and 10.8.24 for cloud implementations. The IRS will continue to ensure compliance with the documented cloud security control infrastructure for increased Cloud Service Provider key management monitoring, including enhancement of audit trails.

PCA Implementation Due Date: October 15, 2024

PCA Status: Open as of July 19, 2024

October 30, 2023

The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement

Report Number 2024-200-005

Recommendation 1: The Chief Information Officer should implement a method of mapping Office of Management and Budget Memorandum M-21-31 requirements for all IRS systems to track and demonstrate compliance.

IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will complete implementation of the automatic tracking tool to demonstrate compliance with Office of Management and Budget Memorandum M-21-31, which the IRS is in the process of doing.

PCA Implementation Due Date: March 15, 2024

Modified Due Date: March 15, 2025

PCA Status: Open as of July 19, 2024


Recommendation 2: The Chief Information Officer should develop and implement a plan to ensure that event logging data are collected from all systems that contain PII and FTI in accordance with IRM requirements.

IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will consolidate the IRS's plans, directives, and process documentation into a formal event logging plan to communicate its delivery strategy for addressing auditing requirements.

PCA Implementation Due Date: March 15, 2024

PCA Status: Closed on March 14, 2024

Recommendation 3: The Chief Information Officer should direct a taxonomy reconciliation effort across the enterprise to standardize the IRS taxonomy to ensure that the Next Generation Enterprise Security Audit Trails program has a complete and accurate inventory of systems for its data repository.



IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, and the Associate Chief Information Officer, Enterprise Services, will collaborate with the Privacy, Governmental Liaison, and Disclosure office to standardize the information system taxonomy across the IRS to reduce the complexity of their manual reconciliation efforts.

PCA Implementation Due Date: September 30, 2024

PCA Status: Open as of July 19, 2024

Recommendation 4

The Chief Information Officer should ensure that the Next Generation Enterprise Security Audit Trails program periodically validates receipt of required audit trail data from all source systems.

IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will document receipt of audit trail data from all source systems.

PCA Implementation Due Date: March 15, 2024

PCA Status: Closed on March 14, 2024

Recommendation 5: The Chief Information Officer should ensure that user inactivity on its data repository is monitored, and actions are taken on user accounts in accordance with the IRS Cloud Computing Security Policy IRM requirements.

IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will automate the disablement of inactive user accounts in accordance with IRM policies and procedures. This will move them from a manual, cyclical process to an automated real-time process.

PCA Implementation Due Date: March 15, 2024

Modified Due Date: June 15, 2024

PCA Status: Closed on June 10, 2024

Recommendation 6: The Chief Information Officer should ensure that user access is authorized for the two modules containing audit trail information in accordance with IRS mission and business functions.

IRS Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will restrict the eligibility requirements for user access to the two modules identified by TIGTA with an added layer of approval by the Cybersecurity organization. The IRS has implemented annual recertification procedures to ensure that continued authorization is appropriate.

PCA Implementation Due Date: March 15, 2024

PCA Status: Closed on March 14, 2024

Glossary of Terms

Term	Definition
Applications	A software program hosted by an information system.
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Contractors	Contractors are individuals external to the IRS that supply goods and services according to a formal contract and task order. These services may include cybersecurity and information technology consulting.
Exempt Organizations	An IRS function that administers tax law governing charities, private foundations, and other entities exempt from Federal income tax.
Form 990-T, <i>Exempt Organization Business Income Tax Return</i>	An information return used by tax exempt organizations to report unrelated business income and tax liabilities with the IRS.
Joint Audit Management Enterprise System	The Department of the Treasury system for use by all bureaus to track, monitor, and report the status of internal control audit results. The system tracks specific information on issues, findings, recommendations, and the PCAs from audit reports issued by oversight agencies, such as TIGTA.
Joint Statistical Research Program	A part of Statistics of Income, which is a division of the RAAS organization. The program seeks to enable the use of tax microdata by qualified researchers outside the Federal Government.
Non-Privileged Access	Access to a server via an application, or an application's graphical user interface which does not login to the operating systems level is not considered privileged access.
Office of Tax Analysis	Analyzes the effects of the existing tax law and alternative tax programs and prepares a variety of background papers, position papers, policy memoranda, and analytical reports on economic aspects of domestic and international tax policy.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of PII are name, Social Security Number, date of birth, place of birth, address, and biometric record.
Privileged Access	A right granted to an individual, a program, or a process.
Research, Applied Analytics, and Statistics	The IRS's centralized research and analytic organization. RAAS partners with embedded research functions to share information and analytic techniques to collaborate on projects and identify learning and training opportunities.

Term	Definition
Security Summit	The IRS formed the Security Summit with representatives from States' Department of Revenue, the Chief Executive Officers of leading tax preparation firms, software developers, and payroll and tax financial product processors. 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.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
System Interconnection	The direct connection of two or more information technology systems for the purpose of sharing data and other information resources.
Treasury Security Operations Center	The Treasury Security Operations Center deploys new enterprise-wide and department-wide security capabilities, or integrates those already in place, as appropriate, to strengthen the overall protection of the enterprise and department.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.

Abbreviations

BEARS	Business Entitlement Access Request System
CDW	Compliance Data Warehouse
FTI	Federal Tax Information
FY	Fiscal Year
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
JAMES	Joint Audit Management Enterprise System
PCA	Planned Corrective Action
PII	Personally Identifiable Information
RAAS	Research, Applied Analytics, and Statistics
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access, Attempted Access, or Inspection of Taxpayer Records



**To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at
oi.govreports@tigta.treas.gov.**

**To make suggestions to improve IRS policies, processes, or systems
affecting taxpayers, contact us at www.tigta.gov/form/suggestions.**

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