TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Compliance Data Warehouse Security Needs Improvement

September 9, 2024

Report Number: 2024-200-042

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

HIGHLIGHTS: Compliance Data Warehouse Security Needs Improvement

Final Audit Report issued on September 9, 2024 **Report Number 2024-200-042**

Why TIGTA Did This Audit

The primary goal of the Compliance Data Warehouse (CDW) is to provide a single, integrated environment of data and computing services to support the research and analysis needs of IRS employees and research analysts. The CDW offers a broad range of databases that authorized research analysts may access through a variety of data analytic tools.

This audit was initiated to determine whether sufficient security safeguards over the CDW exist to protect taxpayer data against unauthorized access.

Impact on Tax Administration

The IRS is required to record audit trails in the system's security documentation for indications of inappropriate or unusual activity. By failing to timely review the CDW's actionable audit events, unauthorized access to sensitive taxpayer data and Personally Identifiable Information could be occurring without detection. In addition, the IRS is required to report identified information security weaknesses and document remediation. Failure to remediate vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

What TIGTA Found

Since August 2022, the CDW's audit trails have been sent to the agency's audit trail repository. However, the tools used to visualize the audit trails failed to accurately display a login data field, resulting in incomplete and unreliable login data.

The current process used to review, analyze, and report on required audit event types is an inefficient and manual process that requires employees responsible for reviewing, analyzing, and reporting on the audit trails to view singular audit events. Also, the agency's audit trail repository is not configured to allow automated notifications for audit events that require escalation.

The CDW [redacted] From December 2022 to October 2023, nine Plans of Action and Milestones were created to implement corrective action plans for the [redacted] vulnerabilities. However, none of the Plans of Action and Milestones were created within agency-defined timelines. During the audit, the IRS updated all active CDW Plans of Action and Milestones to be compliant with agency security policies.

[redacted]

What TIGTA Recommended

TIGTA recommended that: 1) the Chief Data and Analytics Officer ensure that the agency's audit trail repository accurately displays and reports all CDW login information; 2) the Chief Information Officer ensure that all required actionable audit events for the CDW are reviewed; 3) the Chief Information Officer ensure that automated mechanisms are incorporated into the actionable audit event escalation process; 4) the Chief Information Officer and Chief Data and Analytics Officer ensure that identified vulnerabilities are timely remediated; and 5) the Chief Data and Analytics Officer ensure that all CDW servers are included in configuration compliance scans.

The IRS agreed with all five recommendations. The Chief Data and Analytics Officer plans to develop a procedure to periodically verify that the agency's audit trail repository accurately displays and reports all login information for the CDW; modify existing procedures to support timely vulnerability remediation; and implement configuration scans using the agency's prescribed enterprise scanning system(s). In addition, the Chief Information Officer plans to review CDW actionable audit events and seek additional ways to incorporate automated processes to enhance actionable audit event escalations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 9, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

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

SUBJECT: Final Audit Report – Compliance Data Warehouse Security Needs Improvement (Audit No.: 202320017)

This report presents the results of our review to determine whether sufficient security safeguards over the Compliance Data Warehouse exist to protect taxpayer data against unauthorized access. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included in Appendix III. If you have any questions, please contact me or Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

The mission of the Internal Revenue Service (IRS) is to provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all. During Fiscal Year 2023, the IRS collected nearly $4.7 trillion in gross taxes, processed almost 271.5 million tax returns and other forms, and issued about $659 billion in tax refunds.[1] Lastly, IRS.gov received more than 880.9 million visits and taxpayers downloaded about 538.1 million files. To support these efforts, the IRS relies extensively on information technology to process tax returns, collect taxes, distribute tax refunds, and carry out many other services for taxpayers.

The mission of the Research, Applied Analytics, and Statistics (RAAS) organization is to lead a data driven culture through innovative and strategic research, analytics, statistics, and technology services to support effective and efficient tax administration in partnership with internal and external stakeholders. The Chief Data and Analytics Officer leads the RAAS organization and reports directly to the Chief Operating Officer. To accomplish its mission, the RAAS organization is the owner of a system that contains several subsystems, one of which is the Compliance Data Warehouse (CDW). According to the IRS, the primary goal of the CDW is to provide a single, integrated environment of data and computing services to support the research and analysis needs of IRS employees and research analysts. The CDW is not a traditional computer software application. At its core, the CDW is a massive data warehouse containing multiple years of Federal Tax Information and Personally Identifiable Information consolidated from multiple sources, internal and external to the IRS. The CDW offers a broad range of databases that research analysts may access through a variety of data analytic tools. Examples of the data available include:

- Individual Master File data.
- Business Master File data.
- Tax return data.
- Taxpayer contact information.
- Conversations between a taxpayer and an IRS agent.
- Actions that took place on behalf of the IRS.

The CDW is specifically designed to meet the unique needs of research analysts throughout the IRS and other Department of the Treasury (hereafter referred to as the Treasury Department) functions. The CDW captures data from multiple production environments, migrates the data to the CDW environment, and organizes the data in a way that is conducive to analysis. Besides delivering data, the CDW also provides software tools and computing services to support research projects, analysis, and extensive studies. Authorized users can remotely access the CDW and its data only through a secure virtual private network connection and are able to download data extracts to their IRS provided workstations or laptops.

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

The CDW offers a range of solutions to its community of researchers that include:

- Data integration – consolidating data from a variety of sources for research and analysis capabilities.
- Data transfer – making the data within the CDW accessible through various tools used on behalf of CDW customers.
- Data modeling – modifying the presentation of the data so that users can effectively extrapolate the data for their purposes.

As of September 2023, the CDW had 1,173 users including 755 IRS employees, 291 contractors, 74 other Federal agency employees, and 53 unpaid hires (researchers and student volunteers). There were 254 users who had access to masked data and 919 users who had access to unmasked data. Masked data contains no Personally Identifiable Information, while unmasked data includes Personally Identifiable Information. Access to either kind of data requires an approved access entitlement, and access to Personally Identifiable Information also requires executive level approval. Figure 1 provides a summary of CDW users by type of user with access to masked and unmasked data.

Figure 1: Summary of Users With CDW Data Access

	IRS EMPLOYEES	CONTRACTORS	OTHER FEDERAL EMPLOYEES	UNPAID HIRES
CDW Users	755	291	74	53
Unmasked Access	587	239	73	20
Masked Access	168	52	1	33

78 percent of approved CDW users have access to unmasked data.

Source: Treasury Inspector General for Tax Administration's (TIGTA) analysis of the CDW's approved user list and entitlements.

Results of Review

Audit Trail Data Is Sent to the Repository; but, Accurate Login Information Is Not Always Accessible

We found that since August 2022, the CDW's audit trails have been sent to the agency's audit trail repository and that eight required data fields are captured in support of the audit function.

Figure 2: Required Audit Trail Data Fields

Data Field	CDW Audit Trails Satisfy Requirement
Time Stamp	Yes
User Type	Yes
User ID	Yes

Data Field	CDW Audit Trails Satisfy Requirement
End-user Workstation	Yes
Event ID[2]	Yes
Tax Filer Taxpayer Identification Number	Not Applicable
Event Type	Yes
System	Yes
Return Code	Yes

Source: TIGTA's analysis of the CDW's audit trails and the IRS's unauthorized access failed audit assessment document.[3]

However, we determined that the tools used to visualize audit trails associated with the Event ID [identification] data field, specifically CDW logins, failed to accurately display the login data field, with the result that the available login data were both incomplete and unreliable. For example, we found that from March 2023 to July 2023, the repository was not displaying any audit trails that contained CDW login information.[4]

Per the Internal Revenue Manual (IRM), host systems are required to send system audit trails to the agency's repository.[5] Also, according to agency security policies, there are nine required data fields for each audit trail file but only eight are applicable to the CDW.

The CDW login information in the agency's audit trail repository is not always complete and reliable because of two root causes:

- Error with the coding script: Within the CDW Platform Audit Worksheets, the coding script used to identify system logins in the CDW logs was referencing an incorrect file name. Upon recognizing the error, RAAS management officials alerted the appropriate Cybersecurity officials and continue to collaborate to identify and implement a resolution.
- Search periods of more than 90 days: When the login information search period is greater than 90 days, the search does not return complete and accurate login information. However, according to the IRS, search periods that are less than 90 days will provide all user login information. As of April 3, 2024, the exact cause of this error is still unknown; however, Cybersecurity officials continue to troubleshoot the issue. The IRS reports that restricting the search to 90 days or fewer helps manage performance and response time, given the sheer volume of CDW log data. The IRS plans to add a note to the audit trail repository to advise about the 90-day limitation and notes that multiple searches for 90 days or fewer may be run.

[2] One of the Event ID [identification] types includes system logins.

[3] IRS, *Security Audit and Analysis System Failed Audit Log Assessment,* Ver. 3.0 (Apr. 2017).

[4] Due to unreliable login information data displayed, we were unable to properly evaluate CDW user accounts.

[5] [redacted]

Failure to accurately and reliably report system login information limits audit capability to determine access to Personally Identifiable Information and Federal Tax Information data and the ability to identify root causes of information system problems.

Recommendation 1: The Chief Data and Analytics Officer should ensure that the agency's audit trail repository accurately displays and reports all CDW login information.

Management's Response: The IRS agreed with the recommendation. During the course of the audit, the Chief Data and Analytics Officer ensured that all CDW login information can be displayed and reported and is developing a procedure to periodically verify that the agency's audit trail repository continues to accurately display and report all CDW login information in the enterprise audit trail repository.

The Process for Reviewing Actionable Audit Events Is Inefficient and Lacks Automated Mechanisms

The Compliance and Audit Monitoring team within the Cybersecurity function's Counter Insider Threat Operations organization is responsible for the review, analysis, and reporting of actionable audit events for 141 IRS tax systems and applications. In November 2023, we requested information regarding the team's completion of the required review, analysis, and reporting on the audit trail activity. Based on the information provided, we determined that the Compliance and Audit Monitoring team is not reviewing any of the required actionable events, *i.e.*, actionable events require timely review to determine if additional escalation or notifications are required.

The IRM requires that audit trails be reviewed and analyzed at a frequency in accordance with a risk-based decision. The audit trails must be recorded in the system's security documentation for indications and potential impact of inappropriate or unusual activity. Per agency security policies, [redacted][6] Lastly, per the IRM, automated mechanisms shall be used to integrate audit review, analysis, and reporting processes. A management official stated that CDW's actionable events are not being reviewed because of a miscommunication between the Compliance and Audit Monitoring team and CDW personnel, and that the team will begin the review of all required actionable audit events in March 2024.

The audit trails have been available in the agency's repository since August 2022, and as of December 2023, [redacted] The Compliance and Audit Monitoring team has been reviewing the CDW's audit events (non-actionable) related to search queries since August 2023. In addition to not reviewing, analyzing, and reporting on the actionable events, we found the current process for these audit events and actionable events from other IRS tax systems and applications to be [redacted]

[6] [redacted]

During discussions with the Compliance and Audit Monitoring team, several root causes were identified as key contributors to the inefficiency of the review, analysis, and reporting process, including:

- The inability to export all audit events into a single file.
    - The IRS's audit trail repository does not permit users to export or download multiple auditable or actionable events at the same time. As a result, the team is restricted to reviewing, analyzing, and reporting on singular audit events. We met with IRS officials to discuss the lack of automated mechanisms used in the process. Cybersecurity officials stated that they had received a request in January 2024 from the Counter Insider Threat Operations organization to implement the capability of exporting multiple audit events into a single file.

[redacted]

    - [redacted]
    - [redacted]

Management Action: In response to this finding, in May 2024, the capability to allow multiple auditable and actionable events to be exported at the same time into a single file was implemented. However, no action was taken to address the lack of automation for the escalation process.

By failing to timely review the CDW's required actionable audit events, unauthorized access to sensitive taxpayer data and Personally Identifiable Information could be occurring without detection.

The Chief Information Officer should ensure that:

Recommendation 2: The Compliance and Audit Monitoring team is reviewing all required CDW actionable audit events.

> **Management's Response:** The IRS agreed with the recommendation. The Cybersecurity, Counter Insider Threat Operations function plans to review CDW actionable audit events.

Recommendation 3: Automated mechanisms are incorporated into the actionable audit event escalation process.

> **Management's Response:** The IRS agreed with the recommendation. The Cybersecurity, Counter Insider Threat Operations function plans to seek additional ways to incorporate automated processes to enhance actionable audit event escalations where manual processes currently exist.

Process Improvements Have Been Made; but, Several Active Plans of Action and Milestones Were Noncompliant With Minimum Agency Security Requirements

In September 2023, we identified 14 active CDW Plans of Action and Milestones (POA&M). Active POA&Ms are those with a status of either In Progress, Late, or Completed. We determined that 12 (86 percent) of the 14 active POA&Ms were in Late status, while the remaining two were classified as In Progress. We also determined that seven (50 percent) of the 14 active POA&Ms were noncompliant with agency security policies because they lacked required status/progress comments, had insufficient documentation to justify a modified POA&M due date, or did not have required due date comments. The remaining seven active POA&Ms were compliant with agency security policies.

The Federal Information Security Modernization Act of 2014 (FISMA) mandates that all Federal agencies develop and implement a corrective action plan, *i.e.*, a POA&M, to identify and document the resolution of information technology security weaknesses.[7] The IRS uses the Treasury FISMA Inventory Management System tool to manage the collection and reporting of information associated with the FISMA. System owners are required to report identified weaknesses for FISMA classified systems in the tool to identify, track, and manage information technology weaknesses along with documenting remediation efforts.

The IRM requires POA&M status/progress comments to be updated, at a minimum, on a quarterly basis. In addition, agency security policies state that when business units revise the POA&M due date, comments are required and should address the reason for the inability to timely close the POA&M and explain how the revised due date was determined.[8] Once a POA&M is in a Late status, due date comments are required on a quarterly basis.

RAAS management officials stated that when these POA&Ms were initially created, they did not have the organizational structure in place to provide adequate oversight of the FISMA process, to include managing POA&Ms. For example, when the older POA&Ms were initially created, RAAS did not have specific policies and procedures dedicated to POA&M management. In addition, RAAS was limited to only one employee dedicated to FISMA-related issues. Lastly, RAAS management officials stated they are confident that with the additional employees and the newly implemented internal processes they will be able to provide adequate oversight of the POA&M process and satisfy agency POA&M security policies. Extensions of configuration and vulnerability remediation timelines lengthen the period of exposure of critical tax systems, which may provide expanded opportunities for threat actors to access and exploit data.

Management Action: We verified that from October 2023 to December 2023, RAAS officials made updates in the Treasury FISMA Inventory Management System tool for each of the seven noncompliant CDW POA&Ms. In addition, two of the 14 POA&Ms were validated for closure and are no longer considered active. As a result, all active CDW POA&Ms are now compliant with agency security policies.

[7] 44 U.S.C. § 3551, et seq. (2018).

[8] IRS, *Enterprise FISMA POA&M Standard Operating Procedures*, Ver. 11 (Jan. 2024).

Actions taken to address previously reported CDW POA&M issues

In August 2022, while performing analysis for a previous TIGTA report, we found that 140 (88 percent) of 160 active RAAS POA&Ms were classified as Late.[9] The remaining 20 POA&Ms were classified as In Progress or Completed. Of the 160 active POA&Ms, 44 were specific to the CDW, while 116 were related to other RAAS subsystems. We found that 39 (89 percent) of the 44 were classified as Late. The remaining five CDW POA&Ms were classified as In Progress. We identified the following root causes as key contributors to the late resolution of information security weaknesses within the RAAS organization:

- No business unit specific POA&M remediation procedures.
- Only 1.5 employees assigned to solving technical issues related to POA&Ms.
- Funding challenges delayed the hiring of additional technical employees.

In Calendar Year 2023, RAAS implemented several new internal processes to better manage FISMA-related activities such as closing older POA&Ms, implementing a new biweekly POA&M remediation status meeting, and establishing monthly meetings with the Chief Data and Analytics Officer to discuss tracking and managing information security remediation activities. From January 2023 through July 2023, RAAS hired five new employees dedicated to FISMA and POA&M related activities. As a result, in Calendar Year 2023 RAAS closed 93 POA&Ms including 52 that were initially created in 2018 or earlier.

[redacted]

- [redacted][10]

[redacted]

[9] TIGTA, Report No. 2023-20-042, *Security Weaknesses Are Not Timely Resolved and Effectively Managed* (Aug. 2023).

[10] [redacted]

Figure 3: [redacted]

[redacted]

According to the IRS, the timely identification and resolution of information security weaknesses are the primary cornerstones of a sound information security program. The IRM requires system owners to employ vulnerability scanning tools that look for software flaws and improper configuration settings and measure vulnerability impacts. [redacted]

The Department of Homeland Security states that each vulnerability found on a network should be given a numeric score, meant to represent the risk of not mitigating that vulnerability.[11] Vulnerabilities with the highest risk shall be prioritized and remediated first. The Common Vulnerability Scoring System scores provided by the scanning tools shall be used to prioritize vulnerabilities. Figure 4 shows the risk levels and their associated remediation time frames.

Figure 4: Vulnerability Severity Rating Scale and Remediation Time Frames

Risk Level	Remediate Vulnerability Within
Critical	30 days
High	90 days
Medium	120 days
Low	180 days

Source: TIGTA's analysis of [redacted]

From December 2022 to October 2023, nine POA&Ms were created to implement corrective action plans for the [redacted] untimely unremediated vulnerabilities within the CDW. However, we found that none of these nine POA&Ms were created within agency-defined timelines.

[11] Department of Homeland Security, *Continuous Diagnostics and Mitigation, Agency-Wide Adaptive Risk Enumeration Technical Design Document* (Nov. 2017).

The National Institute of Standards and Technology provides guidance related to developing and updating a POA&M to document the planned remediation actions to reduce or eliminate known vulnerabilities in the system.[12] In addition, agency security policies require that all new information security weaknesses be entered into appropriate POA&Ms within 60 days of the initial identification of the weakness.

RAAS management officials acknowledged [redacted] In response, RAAS officials stated that it has been challenging to manage POA&Ms during the IRS's transition of enterprise vulnerability scanning tools.[13] Lastly, RAAS management officials stated that because of the hiring of the additional employees from January through July 2023, there are now technical staff dedicated to managing the configuration settings, POA&Ms, and vulnerability remediation processes, to include providing technical support to system administrators responsible for configuration compliance and patch management issues. Failing to timely create corrective action plans and remediate existing vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

Recommendation 4: The Chief Information Officer and Chief Data and Analytics Officer should develop procedures to ensure that identified vulnerabilities are timely remediated as required, and, if the required remediation time frame cannot be met, corrective action plans for unremediated vulnerabilities should be timely created based on agency security policies.

> **Management's Response:** The IRS agreed with the recommendation. The Chief Data and Analytics Officer established POA&Ms to document all vulnerabilities that were overdue for remediation as noted in the report and is developing procedures to support timely vulnerability remediation. In addition, the Chief Data and Analytics Officer is modifying existing internal POA&M management procedures to document the process for establishing POA&Ms when extenuating circumstances prevent vulnerabilities from being remediated within the policy time frame.

Multiple servers were not in compliance with configuration requirements

We reviewed a configuration compliance scan report dated September 5, 2023, and found that it included [redacted] CDW servers. [redacted] The remaining 13 servers were compliant with agency security policies. [redacted]

[12] National Institute of Standards and Technology, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

[13] From August 2022 to August 2023, the IRS transitioned to a new enterprise vulnerability scanning tool. In August 2023, the new scanning tool became the official system of record.

Management Actions: In response to this finding, from September 2023 to November 2023, RAAS officials successfully remediated [redacted] failed high-risk checks. We reviewed a November 2023 configuration compliance scan report and validated that these six findings no longer appeared on the report. The IRS created an active POA&M for the remaining [redacted]. In addition, in September 2023, RAAS officials acknowledged that [redacted] were not included in the configuration scans and stated that system administrators resolved the issue. We verified that [redacted] servers are now included on the configuration compliance scan reports, [redacted]

[redacted] The IRS uses a configuration setting scanning tool to scan for configuration compliance that transmits the results to a dashboard for review. Lastly, per the IRS user guide, [redacted]

Similar to the previous finding, this issue was due to the lack of existing internal processes specific to configuration settings and a lack of technical staff to manage FISMA-related activities. Failing to keep servers in compliance with configuration requirements compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

Recommendation 5: The Chief Data and Analytics Officer should develop procedures to ensure that all CDW servers are included in configuration compliance scans as required.

Management's Response: The IRS agreed with the recommendation. The Chief Data and Analytics Officer plans to develop a policy and procedures to implement configuration scans using the agency's prescribed enterprise scanning system(s) when CDW hosts are provisioned and plans to conduct regular internal audits to confirm configuration scans meet that policy.

All Users Completed Required Security and Privacy Literacy Training; but, Process Improvements Are Needed

We determined that all 1,173 CDW users as of April 2024 completed each of the four mandatory training courses. Per the IRM, Security and Privacy literacy training shall be provided to all system users and be completed within the following specified time frames:

- As part of initial training for new users and annually thereafter.
- Within five days of being granted access to an IRS system.
- Within 60 days of being granted access to an IRS system, if the user reviews and accepts the IRS's rules of behavior within five days of being granted access.

Figure 5 provides a summary of the four mandatory Security and Privacy literacy training courses that we evaluated as part of our review.

Figure 5: Mandatory Security and Privacy Literacy Training Courses

Source: IRS, FISMA Annual IRS Cybersecurity Awareness Training Standard Operating Procedure, Ver. 1.4 (Jan. 2023).

The Integrated Talent Management system is the IRS's system of record for the administration, documentation, tracking, and reporting of all training completed by all agency employees and contractors. However, within the RAAS organization, mandatory training requirements for unpaid hires (academic researchers and student volunteers) were not managed via the Integrated Talent Management system. According to management officials from the IRS's Human Capital Office, this limitation was due to an integration issue within the agency's human resources system. As a result, senior management within the RAAS organization oversaw the mandatory training requirements process for unpaid hires. This process includes maintaining an internal SharePoint site and providing e-mail notifications to the unpaid hires.

While we found that the current manual process for tracking training requirements for unpaid hires is functional, it does not afford any type of verification that the training was actually completed. For example, as part of the current manual process, unpaid hires provide confirmation of training completion via both e-mail and signed completion forms. RAAS management officials acknowledged that the e-mail responses do not provide any type of verification of training completion. Lastly, we also reviewed RAAS's process for separating unpaid hires at the completion of their projects and found that unpaid hires were timely separated within agency-defined policies and procedures.

In January 2024, we met with officials from both the Treasury Department and the IRS's Human Capital Office to discuss the current system limitations that were preventing the training requirements for unpaid hires to be managed via the Integrated Talent Management system. During this meeting, Treasury Department officials stated that they had received a change request from the IRS specific to this issue with a requested delivery date of April 2024. Treasury Department officials stated that while they anticipate that the change request will be approved, they are unable to project a completion date due to complexity of the change request process and associated funding.

Without an integrated agency-wide system for tracking the completion of required Security and Privacy Awareness training, CDW users may not be fully educated or trained to perform their cybersecurity-related duties and responsibilities consistent with policies, procedures, and agreements.

Management Action: In April 2024, Treasury Department officials confirmed that the change request that will allow the training requirements for unpaid hires to be tracked within the Integrated Talent Management system was successfully deployed.

The Platform Audit Worksheets Satisfy Minimum Agency Security Requirements

We found that the CDW's Platform Audit Worksheets satisfy minimum agency auditing requirements. We analyzed the Platform Audit Worksheets, source system audit trail files, the agency's audit trail repository, and other pertinent system security documents to evaluate compliance with auditing requirements.

Per the IRM, IRS systems must be capable of logging the identity of each user accessing or attempting to access a system; information that establishes what type of event occurred; the source and outcome of the event; the time and date of the access and the logoff; activities that might modify, bypass, or negate security safeguards; security-relevant actions associated with processing; a user generation of reports and extracts containing information categorized as High or Moderate for confidentiality; and other IRS-defined event types documented in system security documentation. The IRS must also provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of incidents and review and update event types selected for logging every two years.

In response to these requirements, the Cybersecurity Architecture and Implementation function's Cybersecurity Solutions Development organization develops platform audit worksheets for all IRS systems and applications. The purpose of the CDW's Platform Audit Worksheets is to assist the Enterprise Operations and Cybersecurity functions with the following:

- Understand which system events are associated with significant security risk (actionable events).
- Log, capture, and deliver audit data to the agency's repository.
- Analyze and report on event trends.

The IRS Addressed a Prior Audit Recommendation to Ensure That Databases Are Timely Patched

In a prior audit, TIGTA found that RAAS is responsible for three database instances.[14] These databases were not timely patched due to various reasons including reliance on vendor patches that are bundled and an incorrect assumption that the database was covered by a documented risk-based decision. TIGTA recommended that these databases be patched or upgraded to the latest version or appropriately document risk acceptance with a risk-based decision. In October 2023, we requested evidence to support that all RAAS/CDW databases are being timely patched or upgraded to the latest version. Based on the information the IRS provided, we determined that the IRS's Planned Corrective Actions used to timely patch databases successfully met the intent of our original recommendation. RAAS performs database [redacted] on all their databases, including the CDW. The scan report provides any missing patch information on the database server. If a database server is missing a patch, RAAS officials work with the database administrators to install the patch.

[14] TIGTA, Report No. 2022-20-065, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls* (Sept. 2022).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether sufficient security safeguards over the CDW exist to protect taxpayer data against unauthorized access. To accomplish our objective, we:

- Determined the effectiveness and compliance of the process for documenting and remediating information security weaknesses within the CDW by reviewing relevant National Institute of Standards and Technology and IRM guidance, analyzing vulnerability and configuration compliance scans, interviewing members of the RAAS organization and the Cybersecurity function, and evaluating whether CDW POA&Ms are being created and reviewed timely.
- Determined whether the IRS addressed a prior audit recommendation in TIGTA, Report No. 2022-20-065, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls* (Sept. 2022), by evaluating the new process and Planned Corrective Actions used to timely patch databases.
- Determined whether CDW users have completed all mandatory training requirements by reviewing Federal and agency guidance related to Security and Privacy Awareness Training and evaluating Integrated Talent Management system training records.
- Determined whether complete and accurate audit trail data were being sent to the agency's repository by interviewing IRS personnel responsible for the audit trail systems and process, reviewing audit trail policies and procedures, and accessing the audit trail repository.
- Determined the effectiveness and compliance of the CDW's Audit and Accountability policies by reviewing pertinent CDW system security documents, reviewing CDW's Platform Audit Worksheets, and evaluating the required data fields captured in the source system audit trail files.
- Determined whether the CDW's audit trails are reviewed, analyzed, and reported for indications of inappropriate or unusual activity by interviewing members of the Cybersecurity function, reviewing audit trail policies and procedures, evaluating evidence provided by the IRS, and accessing the audit trail repository.
- Determined whether the IRS uses automated mechanisms to integrate audit review, analysis, and reporting processes by reviewing IRM guidance, interviewing members of the Cybersecurity function about the status of automation efforts, and evaluating the audit trail repository.

Performance of This Review

This review was performed with information obtained from the RAAS organization and the Cybersecurity function located at the IRS National Headquarters in Washington, D.C.; the New Carrollton Federal Building located in Lanham, Maryland; and the Enterprise Computing Center located in Martinsburg, West Virginia, during the period August 2023 through June 2024.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Kasey Koontz, Director; Myron Gulley, Audit Manager; Mike Curtis, Quality Assurance Audit Manager, Joe Dryden, Auditor; Cheryl Joneckis, Information Technology Specialist (Data Analytics); and Laura Christoffersen, Information Technology Specialist (Data Analytics).

Data Validation Methodology

We performed tests to assess the reliability of data from the vulnerability and configuration compliance scan repository and the Treasury FISMA Inventory Management System tool. We evaluated the data by: 1) reviewing existing information about the data and the system that produced them; 2) ensuring that the information was legible and contained alphanumeric characters; 3) reviewing the data to detect obvious errors, duplicate values, and missing data; and 4) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

We also performed tests to assess the reliability of CDW login activity using data from the agency's authorized audit trail repository. We evaluated the data by: 1) performing electronic testing of required data elements; 2) interviewing agency officials knowledgeable about the data; and 3) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined that the login data was both incomplete and inaccurate. As a result, we determined that the data were not sufficiently reliable for purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Federal guidance from the Department of Homeland Security and the National Institute of Standards and Technology and the IRM. We evaluated these controls by interviewing employees from the RAAS organization and the Cybersecurity function, accessing the audit trail repository, assessing POA&Ms, analyzing vulnerability and configuration compliance scans, evaluating user account reports and training records, and reviewing available documentation.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Protection of Resources – Potential; [redacted] (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

We analyzed the September 5, 2023, vulnerability scan report and found [redacted]

Type and Value of Outcome Measure:

- Protection of Resources – Actual; Three servers were not included in the CDW's configuration compliance scans (see Recommendation 5).

Methodology Used to Measure the Reported Benefit:

We reviewed a configuration compliance scan report dated September 5, 2023, and found that it included only [redacted] servers were not included in the configuration scans. RAAS officials acknowledged that the [redacted] servers were not included in the configuration scans, but by September 26, 2023, system administrators resolved the issue. We verified that [redacted] of these servers are now included on configuration scans, while the [redacted]

Appendix III

Management's Response to the Draft Report

RESEARCH, APPLIED ANALYTICS AND STATISTICS

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 19, 2024

MEMORANDUM FOR DANNY R. VERNEUILLE
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Holly A. Donnelly
Acting Chief Data and Analytics Officer

Digitally signed by Holly A. Donnelly
Date: 2024.08.19 17:52:03 -04'00'

SUBJECT: Draft Audit Report – Compliance Data Warehouse Security Needs Improvement - Audit # 202320017

Thank you for the opportunity to review your draft report, "Compliance Data Warehouse Security Needs Improvement." As TIGTA noted, the primary goal of the Compliance Data Warehouse (CDW) is to provide a single, integrated environment of data and computing services to support the research and analytics needs of the Internal Revenue Service. The CDW offers a comprehensive range of databases that authorized users can access using a robust set of data analysis tools, to support a broad range of mission critical projects.

Your report examined security safeguards protecting the CDW. We appreciate your recognition of the many steps we have taken to enhance the CDW security posture as part of our continuous effort to protect taxpayer data. We also appreciate your recognition of the progress our team made in addressing issues as they were identified over the course of this engagement.

We agree that you identified significant deficiencies and appreciate your recognition that during the audit we addressed several. These include ensuring our Plan of Action & Milestones (POA&Ms) are compliant with IRS policy, unremediated vulnerabilities are timely documented via POA&Ms, and that all CDW servers are receiving configuration scans as required. To ensure continued compliance, as documented in our proposed plan of corrective actions, we are modifying existing procedures and developing procedures where none previously existed to prevent recurrence.

We recognize the critical importance of protecting all IRS taxpayer data within CDW and appreciate the valuable feedback and recommendations you have provided. We are committed to continuously improving the protection of taxpayer data. The support, assistance, and guidance your team provided is very valuable to us in this regard. Our corrective action plan for addressing your recommendations is attached. If you have any questions, please contact Barry W. Johnson at (202) 803-9794 or a member of your staff may contact Reza Rashidi at (703) 832-1588.

Attachment

Enclosure

RECOMMENDATION #1:
The Chief Data and Analytics Officer should ensure that the agency's audit trail repository accurately displays and reports all CDW login information.

CORRECTIVE ACTION:
The IRS agrees with the recommendation. During the course of the audit, the Chief Data and Analytics Officer ensured that all CDW login information can be displayed and reported and is developing a procedure to periodically verify that the agency's audit trail repository continues to accurately display and report all CDW login information in the enterprise audit trail repository.

IMPLEMENTATION DATE:
May 31, 2025

RESPONSIBLE OFFICIAL:
Chief Data and Analytics Officer

RECOMMENDATION #2:
The Chief Information Officer should ensure that the Compliance and Audit Monitoring team is reviewing all required CDW actionable audit events.

CORRECTIVE ACTION:
The IRS agrees with the recommendation. Cybersecurity, Counter Insider Threat Operations will review CDW actionable audit events.

IMPLEMENTATION DATE:
February 15, 2025

RESPONSIBLE OFFICIAL:
Chief Information Officer

RECOMMENDATION #3:
The Chief Information Officer should ensure that automated mechanisms are incorporated into the actionable audit event escalation process.

CORRECTIVE ACTION:
The IRS agrees with the recommendation. Cybersecurity, Counter Insider Threat Operations will seek additional ways to incorporate automated processes to enhance actionable audit event escalations where manual processes currently exist.

IMPLEMENTATION DATE:
April 15, 2025

RESPONSIBLE OFFICIAL:
Chief Information Officer

RECOMMENDATION #4:

Enclosure

The Chief Information Officer and Chief Data and Analytics Officer should develop procedures to ensure that identified vulnerabilities are timely remediated as required, and, if the required remediation time frame cannot be met, corrective action plans for unremediated vulnerabilities should be timely created based on agency security policies.

CORRECTIVE ACTION:
The IRS agrees with the recommendation. The Chief Data and Analytics Officer established POA&Ms to document all vulnerabilities that were overdue for remediation as noted in the report and is developing procedures to support timely vulnerability remediation. In addition, the Chief Data and Analytics Officer is modifying existing internal POA&M management procedures to document the process for establishing POA&Ms when extenuating circumstances prevent vulnerabilities from being remediated within the policy timeframe.

IMPLEMENTATION DATE:
March 31, 2025

RESPONSIBLE OFFICIAL:
Chief Data and Analytics Officer

RECOMMENDATION #5:
The Chief Data and Analytics Officer should develop procedures to ensure that all CDW servers are included in configuration compliance scans as required.

CORRECTIVE ACTION:
The IRS agrees with the recommendation. The Chief Data and Analytics Officer will develop a policy and procedures to implement configuration scans using the agency's prescribed enterprise scanning system(s) when CDW hosts are provisioned. To verify continued compliance, regular internal audits to confirm configuration scans meet that policy will be conducted.

IMPLEMENTATION DATE:
July 30, 2025

RESPONSIBLE OFFICIAL:
Chief Data and Analytics Officer

Appendix IV

Glossary of Terms

Term	Definition
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.
Auditable Event	An observable occurrence in the system used to support after-the-fact investigations of incidents.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Business Master File	The IRS database that consists of Federal tax-related transactions and accounts for businesses. These include employment taxes, income taxes on businesses, and excise taxes.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. It attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
Compliance Data Warehouse	An IRS repository of compliance, filing, and related databases that are used to support projects, analyses, and studies related to tax administration.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or functionality of the information system.
Counter Insider Threat Operations	Charged with promoting an IRS operations security mindset and practice, incorporating audit monitoring and risk management based on operations security policy and principle.
Cybersecurity Function	A function within the Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Data Repository	An information library or archive used to collect, manage, or store data sets for analysis and reporting.
Database Instance	A set of memory structure and background processes that access a set of database files.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.

Term	Definition
Federal Information Security Modernization Act of 2014	Amendment to the Federal Information Security Management Act of 2002[15] that allows for further reform to Federal information security. This bill amends Chapter 35 of Title 44 of the United States Code. The original statute (Federal Information Security Management Act of 2002) requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget.
Federal Tax Information	Consists of Federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Integrated Talent Management System	A Treasury Department enterprise system that provides various functions, including a learning management model that delivers training content to employees and contractors.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Masked Data	Removed or replaced aspects of sensitive data that one might trace back to specific taxpayers.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Patch	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are: name, Social Security Number, date of birth, place of birth, address, and biometric record.
Plan of Action and Milestones	A corrective action plan to identify and document the resolution of information security weaknesses and periodically report to the Office of Management and Budget, the Treasury Department, and Congress.

[15] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

Term	Definition
Platform Audit Worksheet	Assists the Cybersecurity and Enterprise Operations functions with ensuring that information systems comply with both Federal and agency security policies related to auditing requirements.
Production Environment	The location where the real-time staging of programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Risk-Based Decision	A decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analyses, assessments, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase, and a decision is made taking the entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis assessments, recommended risk mitigation strategies, and business impact.
Threat Actors	The instigators of risks with the capability to do harm.
Treasury FISMA Inventory Management System	The official FISMA data repository for all Treasury Department bureaus. The data maintained in this repository are used as part of the Treasury Department's efforts to comply with the E-Government Act of 2002[16] as well as National Institute of Standards and Technology and Office of Management and Budget regulations and guidance.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.
Virtual Private Network	A restricted-use computer network that is constructed from the system resources of a network.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.

[16] Pub. L. 107-347, 116 Stat. 2899.

Appendix V

Abbreviations

CDW	Compliance Data Warehouse
FISMA	Federal Information Security Modernization Act of 2014
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones
RAAS	Research, Applied Analytics, and Statistics
TIGTA	Treasury Inspector General for Tax Administration

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.