TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

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

October 30, 2023

Report Number: 2024-200-005

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

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

Final Audit Report issued on October 30, 2023 **Report Number 2024-200-005**

Why TIGTA Did This Audit

In May 2021, the Office of the President of the United States issued Executive Order 14028 on Improving the Nation's Cybersecurity. In August 2021, the Office of Management and Budget (OMB) issued a memorandum on Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. The memorandum established four event logging maturity levels and required Federal agencies to complete implementation by August 2023.

This audit was initiated to determine whether the IRS effectively implemented the Next Generation Enterprise Security Audit Trails (ESAT) program to meet Federal and IRS requirements.

Impact on Tax Administration

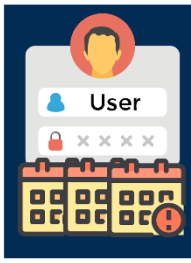
The IRS collects, processes, and stores large amounts of taxpayer information. Recent cybersecurity incidents underscore the importance of increased visibility before, during, and after an incident. Information from audit logs on Federal information systems is invaluable in the detection, investigation, and remediation of cyber threats. Failure to capture and review audit trails for all systems with access to sensitive data prevents the IRS from assuring it can safeguard taxpayer data. In addition, without complete audit trails, unauthorized accesses to sensitive taxpayer data and Personally Identifiable Information could be occurring in IRS systems without detection.

What TIGTA Found

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. 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 the OMB requirements.

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 addition, the IRS is not effectively identifying and tracking all systems and applications to ensure audit trail data are collected in the data repository. In May 2023, TIGTA analyzed the completeness of audit trail records in the IRS's data repository on a judgmental sample of seven systems. TIGTA found that the audit trail data for four of the seven systems were complete, but three of the seven systems had data in its source file that were not in the IRS's data repository.

Finally, the IRS is not properly managing user accounts for its data repository. Specifically, TIGTA 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.



The IRS identified 486 (35 percent) of 1,383 users with access to its data repository that had not logged into the system in 90 days.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer should 1) implement a method of mapping OMB requirements for all IRS systems to track and demonstrate compliance; 2) develop and implement a plan to ensure event logging data are collected as required; 3) direct a taxonomy reconciliation effort across the enterprise to ensure the Next Generation ESAT program has a complete and accurate inventory of applicable systems for its data repository; 4) periodically validate receipt of required audit trail data from all source systems; 5) ensure that user inactivity on its data repository is monitored in accordance with requirements; and 6) ensure that user access is authorized for the two modules containing audit trail in accordance with IRS mission and business functions.

The IRS agreed with all six recommendations and stated that 37 of the 356 previously identified systems did not require application logging. The IRS further stated that by September 30, 2023, it has completed implementing logging requirements on 318 of 319 systems and temporarily removed the remaining legacy system.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

October 30, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Matthew A. Weir
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement (Audit # 202320016)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) effectively implemented the Next Generation Enterprise Security Audit Trails program to meet Federal and IRS requirements. This review was part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources.*

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

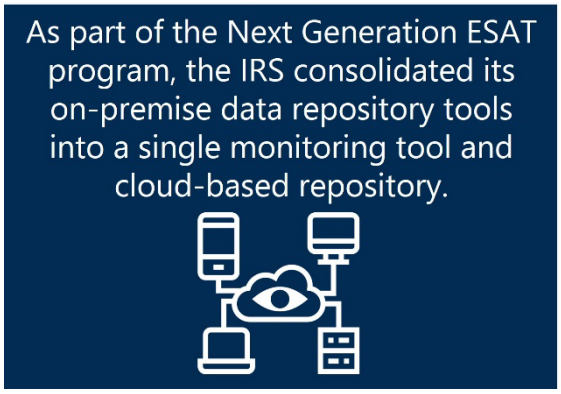
Table of Contents

Appendices

Background

The Internal Revenue Service (IRS) collects, processes, and stores large amounts of taxpayer information. Recent cybersecurity events underscore the importance of increased visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems is invaluable in the detection, investigation, and remediation of cyber threats. An audit trail generally refers to a record of events, called logs, occurring on a computer system.[1] Routine audit trail analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

In March 2010, the IRS established the Enterprise Security Audit Trails (ESAT) program to manage the enterprise audit initiative and oversee the deployment of information technology solutions to resolve systemic audit trail issues. According to the IRS, multiple solutions were implemented over the years, resulting in silos of data with no correlation or visibility across them to meet audit control requirements. The size and scope of the ESAT program has increased significantly over the years. In 2012, TIGTA determined that 14 systems were sending audit trail files to its legacy audit trail system. In 2015, the number increased to 32 systems, with a further increase to 36 in 2020.[2]



In March 2021, the Cybersecurity function documented a strategy to transition from ESAT to Next Generation ESAT to modernize audit capabilities and reduce technical and organizational complexity. According to the IRS strategy, the transition focused on creating a data-focused, enterprise-wide audit management system that centralizes, standardizes, and provides better visibility and analysis capability for audit data from various sources. As part of the Next Generation ESAT program, the IRS consolidated its on-premise data repository tools into a single monitoring tool and cloud-based repository. The program also assists IRS system owners with navigating the collection and processing of computer-generated event logs or audit trails.

In May 2021, the Office of the President of the United States issued an Executive Order on Improving the Nation's Cybersecurity.[3] According to the order, it is essential that agencies and their information technology service providers collect and maintain information from network and system logs on all Federal information systems. In August 2021, the Office of Management and Budget (OMB) issued Memorandum M-21-31 on Improving the Federal Government's

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

[2] Treasury Inspector General for Tax Administration, 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), and Treasury Inspector General for Tax Administration, Report No. 2020-20-033, *Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trail Data to Detect Unauthorized Access to Sensitive Information* (Jul. 2020).

[3] Exec. Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

Investigative and Remediation Capabilities Related to Cybersecurity Incidents.[4] OMB Memorandum M-21-31 established an Event Logging maturity model that includes four tiers and established due dates for Federal agencies to meet the requirements.

Event Logging Tiers:

- Event Logging 0 – Not Effective. Logging requirements of highest criticality are either not met or are only partially met.
- Event Logging 1 – Basic. Requirements include basic data logging categorization, time standards, event forwarding, protecting and validating log information, and basic centralized access. Agencies must reach Event Logging 1 maturity within one year of the memorandum date (August 2022).
- Event Logging 2 – Intermediate. Requirements include meeting all Event Logging 1 maturity requirements, intermediate data logging categorization, publication of standardized log structure, inspection of encrypted data, and intermediate centralized access. Agencies must reach Event Logging 2 maturity within 18 months of the memorandum date (February 2023).
- Event Logging 3 – Advanced. Requirements include meeting all Event Logging 2 maturity requirements, advanced logging categorization, logging automation and response, user behavior monitoring, application container security, operations, and management, and advanced centralized access. Agencies must achieve Event Logging 3 maturity within two years of the memorandum date (August 2023).

According to the IRS, the Next Generation ESAT program supports Executive Order 14028 and OMB Memorandum M-21-31 compliance.

Results of Review

The IRS Has Not Fully Implemented Its Automated Tool for Monitoring Office of Management and Budget Event Logging Requirements

The IRS is currently implementing a tool that will help demonstrate OMB Memorandum M-21-31 compliance. This tool will enable the IRS to organize its infrastructure, apply logging requirements, identify where the IRS meets requirements and where it has gaps, track progress meeting requirements, and demonstrate to auditors that the IRS meets requirements of event logging tiers. As of August 10, 2023, the IRS has not provided a date when the tool will be implemented. The IRS does not have any other tool that can track and demonstrate OMB Memorandum M-21-31 compliance.

The IRS stated that having a tool that maps (*i.e.*, associates specific logging requirements to the implementation status of that requirement within different systems) logging requirements to

[4] OMB, Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 27, 2021).

systems is not a requirement of OMB Memorandum M-21-31. While we agree with this statement, the inability to document and demonstrate compliance with OMB Memorandum M-21-31 requirements creates obstacles for the IRS to show it monitors its compliance and for the independent verification of compliance.

The OMB memorandum required Federal agencies to reach Event Logging 2 by February 2023. Treasury reported that the IRS was only at Event Logging 1 for the 2nd quarter of Fiscal Year 2023, which ended in March 2023. IRS officials stated it met Event Logging 2 requirements by February 2023, but due to a clerical error, it reported Event Logging 1 for the 2nd quarter of Fiscal Year 2023. Therefore, the IRS did not meet OMB required time frames for event logging maturity.

The requirements to meet Event Logging 1 include establishing basic event logging categories, data, and time standards; and Event Logging 2 requirements include all Event Logging 1 maturity requirements and intermediate data logging categories. Additionally, agencies are required to have centralized access and monitoring of event log data and to protect and validate the log information.

Treasury reported that the IRS was at Event Logging 2 for the Federal Information Security Modernization Act of 2014, hereafter referred to as FISMA, reportable systems as of May 2023.[5] However, this is not the totality of IRS information systems and would not meet the Federal requirements. The IRS provided a report of its 192 FISMA reportable systems listed as Event Logging 2 without an accompanying validation that all required log types and formats were collected.

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 the OMB requirements. While the IRS has increased its audit trail efforts, ESAT personnel were unable to provide a mapping of all 702 OMB logging requirements for all its information systems.[6] Without a method to substantiate the IRS's self-reporting, we are unable to confirm their compliance with OMB M-21-31 Event Logging maturity.

According to the IRS, its data repository collects approximately 25 Terabytes of event log data daily. Due to the amount of data collected, coupled with the 702 logging requirements, the IRS has not been able to completely implement its tool. Because the IRS's tool to score and continuously monitor compliance with the OMB memorandum had not been fully implemented, the IRS lacks the capability to track and demonstrate its compliance with OMB Memorandum M-21-31 requirements. By not complying with OMB Memorandum M-21-31, the IRS limits its incident response efforts and defense of Federal information.

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

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will complete implementation of the automatic

[5] Pub. L. No. 113-283.

[6] The IRS analyzed OMB Memorandum M-21-31 and identified 702 requirements.

tracking tool to demonstrate compliance with OMB Memorandum M-21-31, which the IRS is in the process of doing.

All Applications With Personally Identifiable Information and Federal Tax Information Are Not Sending Audit Trails to the Repository, and Systems and Applications Are Not Effectively Identified and Tracked

Audit trail data sent to the data repository are generally accurate

We reviewed source system audit trail files to determine if the seven systems in our judgmental sample were sending all required data fields.[7] We found that five (71 percent) of the seven source systems were sending all required data fields. Two systems did not include one of the nine required data elements. In addition, the IRS has a known issue with one of the seven systems where event log data were truncated approximately 20 percent of the time. The IRS stated that Cybersecurity function personnel have been working with the application team to resolve the issue. We reviewed the Cybersecurity function Standard Operating Procedures and determined that there are nine required data fields for each audit trail file.

All applications with Personally Identifiable Information or Federal Tax Information are not sending audit trails to the repository

The Internal Revenue Manual (IRM) requires audit trails for systems containing Personally Identifiable Information (PII) and Federal Tax Information (FTI).[8] The IRS states it identified 814 systems requiring an assessment of audit trails requirements. The IRS determined that 356 (44 percent) of the 814 systems required application-level audit trails for the detection and investigation of unauthorized accesses of PII and FTI. Our analysis of the 356 systems as of June 2023 shows that:

- 231 (65 percent) of the 356 systems are sending their event log data to the data repository.
- 125 (35 percent) of the 356 systems are not sending their event log data to the data repository.

Migration from the legacy audit trail system to the new data repository is a major undertaking. In addition, as of June 2023, several system owners have not engaged the Next Generation ESAT program's application audit process to have their event log data collected. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Failure to collect event log data limits audit capability to determine access to PII and FTI data and the ability to identify root causes of information system problems.

[7] We randomly selected the seven systems to obtain a diverse selection of systems to review from a population of 219. A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

[8] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (Dec. 13, 2022).

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

Management's 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 their delivery strategy for addressing auditing requirements.

The Next Generation ESAT program is not effectively identifying and tracking all systems and applications with PII/FTI to ensure audit trail data are collected in the data repository

The IRS uses three inventories that list systems and applications with PII/FTI:

- The As-Built-Architecture Current Production Environment (hereafter referred to as the As-Built Architecture).
- The Privacy Impact Assessment Management System (PIAMS). PIAMS is the inventory for systems and applications that collect and use PII.
- The FISMA Master Inventory list, which designates the highest priority systems that are included in the Treasury FISMA Inventory Management System.

ESAT personnel leverage these three disparate lists to create an inventory of IRS systems to be reviewed for application audit trails requirements. This consolidated list is referred to as the ESAT Tracker. We compared the number of systems in the ESAT Tracker in February 2023 with the PIAMS inventory. Due to system naming discrepancies between the two lists, we could not readily reconcile the items. Therefore, we selected a judgmental sample of 10 systems from PIAMS that could not be reconciled to the ESAT Tracker for review.[9]

We found that the Next Generation ESAT program was not tracking the collection of audit trail data for four (40 percent) of the 10 systems reviewed. As a result, the four systems are not sending audit trail data to the data repository. Although the Next Generation ESAT program was able to account for the remaining six systems, our review determined that one system was not yet in production, one system had a different application name than the name in the ESAT Tracker and was sending audit trails, one did not generate event logs, and the other three systems are part of larger systems and were sending their audit trail data by way of those systems.

The IRM states that host systems shall send their logs to the IRS audit trail authorized repository. OMB Memorandum M-21-31 states that event logs should be collected by a component-level event log manager.

The Next Generation ESAT program was not collecting audit trail information for all PII/FTI systems, because its ESAT Tracker did not include all systems that collect and store PII and FTI. The Next Generation ESAT team had an annual process for updating the PII/FTI application inventory, while making manual updates as information becomes available. In April 2023, the

[9] We selected 10 systems that we determined collected and stored PII but also had naming discrepancies. A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

process was updated to add any applications with PII/FTI. The IRS added 15 systems to the ESAT Tracker as of June 2023 through this process.

The IRS stated that taxonomy or naming issues can cause mismatched data across the As Built Architecture, PIAMS, FISMA Master Inventory, and the ESAT tracker. They also stated that each annual inventory provides a reconciliation of inconsistent taxonomies and that the Next Generation ESAT program must conduct significant research to validate the disparate inventories across the IRS. A consistent taxonomy is required to ensure that all systems with access to sensitive data are identified to ensure taxpayer data are safeguarded.

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

Management's 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.

The IRS did not identify source systems required to transmit audit trail records to its data repository

In May 2023, we analyzed the completeness of audit trail records in the data repository. We selected a judgmental sample of seven systems and compared the audit trail files from the source systems for March 1, 2023, against the data in the data repository for each system. We found that:

- Four (57 percent) of the seven systems had complete audit trail data in the data repository.
- Three (43 percent) of the seven systems contained data in its source audit trail file that were not in the IRS's data repository. Specifically:
    - 1,815 (2 percent) of 106,631 source system audit trail records were missing for one system.
    - 1,780 (51 percent) of 3,493 source system audit trail records were missing for a second system.
    - 23 (47 percent) of 49 source system audit trail records were missing for a third system.

OMB Memorandum M-21-31 requires the protection and validation of log information. The IRS has a process for applications to send audit trail files and includes steps to monitor and remediate issues with the expected audit trail file transmission, but it does not validate that all data records from the source systems are successfully transmitting and loading into the IRS's data repository. We inquired if the IRS performed validation periodically to ensure that its data repository was receiving all source system audit trail data. Cybersecurity function officials stated that they did not.

According to Applications Development management officials, the three systems with missing audit trail data were a part of the same Applications Development product suite. During the transition to the IRS's data repository in September 2022, Next Generation ESAT personnel did not configure 10 of the 25 application log servers to forward their data to the data repository. As a result, the three applications in the Applications Development product suite did not send complete audit trail data to the IRS's data repository for a period of nine months. Without complete audit trails, unauthorized accesses to sensitive taxpayer data and PII could be occurring in IRS systems without detection.

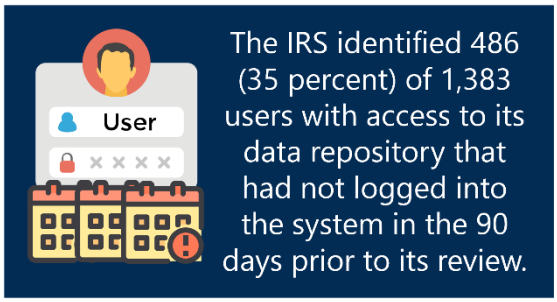
Management Action: As of June 2023, the Next Generation ESAT Program took corrective action to resolve the configuration issue for the 10 log servers and provided documentation showing that all 25 of the affected product suite log servers were sending audit trail data to the data repository.

Recommendation 4: The Chief Information Officer should ensure that the Next Generation ESAT program periodically validates receipt of required audit trail data from all source systems.

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

Data Repository User Accounts Are Not Effectively Managed

The IRS is not removing inactive user accounts timely



The data respository where audit trail information is stored had 1,383 users as of March 2023. The IRS identified 486 (35 percent) of the 1,383 users with access to its data repository that had not logged into the system in the 90 days prior to its March 2023 review.

The IRM requires that information systems be monitored, and inactive user accounts be automatically disabled after 90 calendar days.[10] However, the IRS was not monitoring user activity for its data repository. According to Next Generation ESAT personnel, managing the user accounts for the data repository was complex due to the number of users, approvers, and security requirements.

By not monitoring the activity of user accounts, the IRS is unaware of when inactive accounts reach a threshold that requires action, such as disabling an account or removing access. Failure to properly monitor and deactivate user accounts increases the risk of unauthorized access to sensitive audit trail data.

Management Action: As of June 2023, the IRS implemented an automated process to disable user accounts with 120 days of inactivity. In addition, it began removing access authorizations

[10] IRM 10.8.24, *Information Technology Security, Cloud Computing Security Policy* (Sept. 28, 2021).

to the data repository for user accounts with 120 days of inactivity. While an improvement, the IRS Cloud Computing Security Policy IRM requires inactive user accounts be automatically disabled after 90 calendar days.

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.

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

The IRS is not properly authorizing user access to audit trail information

The data repository that the Next Generation ESAT program uses contains two modules with audit trail information. The Privacy, Governmental Liaison and Disclosure office; the Cybersecurity function's Counter Insider Threat Operations Division; and the Treasury Inspector General for Tax Administration are authorized reviewers of audit trail information for possible IRS policy violations and unauthorized access to taxpayer data. The data repository modules had 74 and 29 authorized users respectively in the Business Entitlement Access Request System as of February 2023. We found that:

Module 1

- 59 (80 percent) of the 74 users had authorization to access Module 1 with a valid business justification
- 15 (20 percent) of the 74 users had authorization to access Module 1 without a valid business justification.

Module 2

- 26 (90 percent) of the 29 users had authorization to access Module 2 with a valid business justification.
- 3 (10 percent) of the 29 users had authorization to access Module 2 without a valid business justification.

The IRM requires the IRS to authorize user access based only on their necessary missions and business functions. Further, sensitive information, such as the PII in these modules, shall be released only to individuals with a duty-driven need-to-know. Each of the 18 users without a business justification worked in business units outside the authorized reviewers. However, the final approvers for the two modules in the data repository rely on first-line management approval to authorize access, regardless of a user's job function. By not properly authorizing user access, the IRS cannot ensure that only users with a proper business justification have access to sensitive data.

Management Action: As of May 2023, each of the 18 users without a valid business justification had their access to the modules removed.

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.

Management's 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.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS effectively implemented the Next Generation ESAT program to meet Federal and IRS requirements. To accomplish our objective, we:

- Determined whether applications were sending complete and accurate audit trail data to the Next Generation ESAT systems by interviewing IRS personnel responsible for the audit trail systems and process, reviewing audit trail policies and procedures, and selecting two judgmental samples.
    - We randomly selected one judgmental sample to obtain a diverse selection of systems to review. The sample contained seven systems from a population of 219 systems and was used to compare source application audit trail files with the audit trail data in the IRS's data repository.[1]
    - We selected one judgmental sample to review systems that collect or store PII and assessed whether they were sending audit trail data to the IRS data repository. The sample contained 10 systems from a population of 85 systems with naming discrepancies between PIAMS and the ESAT Tracker.
- Determined whether the audit trail information in the Next Generation ESAT systems were protected from unauthorized access, modification, and deletion by reviewing authorized users to the Next Generation ESAT systems, assessing whether all users had a valid need-to-know, and reviewing the IRS's process for removing invalid and inactive user accounts.
- Evaluated the Next Generation ESAT program implementation against Federal requirements by interviewing IRS personnel responsible for assessing the event logging maturity level and reviewing documentation of the IRS's current event logging level.

Performance of This Review

This review was performed with information obtained from the IRS's Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland, during the period February through August 2023. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Kasey Koontz, Audit

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Manager; Andrea Nowell, Lead Auditor, Mike Mohrman, Senior Auditor, and Lance Welling, Information Technology Specialist (Data Analytics).

Data Validation Methodology

We performed tests to assess the reliability of data from the IRS data repository, Next Generation ESAT program, and various systems with audit trail data selected from our judgmental sample. 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 also evaluated the accuracy of key data points by reviewing existing policies and procedures and determined if the required data fields were collected. We determined that the data were 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 on Event Logging, IRM guidance, and the ESAT Application Audit Facilitation Standard Operating Procedures. We evaluated these controls by interviewing Information Technology organization personnel, accessing the IRS data repository, reviewing available documentation, and analyzing user account reports.

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; four systems were not sending audit trail data to the IRS's data repository (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental sample of 10 systems with naming discrepancies that were not in the February 2023 ESAT Tracker but collected or stored PII and determined that the IRS was not collecting audit trail data for four of the 10 systems.[1]

Type and Value of Outcome Measure:

- Reliability of Information – Potential; three systems did not have complete audit trail data in the IRS's data repository (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

For a judgmental sample of seven systems, we compared the March 1, 2023, source system audit trail data to audit trail data in the IRS's data repository and determined that the IRS's data repository did not contain all audit trail data for three of the seven systems.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

October 6, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Acting Chief Information Officer

Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2023.10.05 19:40:02 -04'00'

SUBJECT: Draft Audit Report – The IRS Is Not Collecting or Protecting Access to All Audit Trail Data (Audit # 202320016)

Thank you for the opportunity to comment on your draft audit report. The IRS uses a multifaceted approach to protect Personally Identifiable Information (PII) and Federal Tax Information (FTI), including continuous monitoring of audit trails. We have invested significant resources to successfully modernize the IRS Enterprise Security Audit Trails (ESAT) program. This modernization has resolved long-standing technological impediments for the ESAT program.

We have completely modernized the IRS ESAT capabilities by consolidating all audit trails data repositories into a centralized monitoring tool. In March 2022, our ESAT environment was migrated to the Department of the Treasury's Workplace Community Cloud with the highest FISMA/FedRAMP certification. We now have a data-focused, enterprise-wide audit management system that centralizes, standardizes and provides better visibility and analytical capabilities. In October 2022 and December 2022, we further expanded our ESAT cloud-hosted environment to accommodate significantly increased audit trails collection.

Continuous improvement is the cornerstone of all IRS data security programs. As such, we appreciate your recommendations and have attached our corrective action plan. The IRS made order of magnitude improvements in a short time because funding became available.

IRS started with an identified 356 applications that required audit trails. We determined that 37 applications did not require application audit trails and removed them, leaving us 319 applications. By September 30, 2023, we completed audit trails on 318 applications and temporarily removed one application from the network as it is a legacy system that will require additional work to resolve before audit trails will function on this application.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Andrea Beachy, Director, IT Cybersecurity Architecture & Implementation at (703) 980-5299.

Attachment

2

Attachment

Audit# 202320016, The IRS is Not Collecting or Protecting Access to All Audit Trail Data

Recommendations

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

CORRECTIVE ACTION 1: We agree with this recommendation and will complete implementation of the automatic tracking tool to demonstrate compliance with OMB Memorandum M-21-31, which the IRS is in the process of doing.

IMPLEMENTATION DATE: December 29, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

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

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. We will consolidate the IRS plans, directives, and process documentation into a formal event logging plan to communicate our delivery strategy for addressing auditing requirements.

IMPLEMENTATION DATE: December 29, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 3: The Chief Information Officer should direct a taxonomy reconciliation effort across the enterprise to standardize the IRS taxonomy to ensure the Next Generation ESAT program has a complete and accurate inventory of applicable systems for its data repository.

CORRECTIVE ACTION 3: We agree with this recommendation. We will collaborate with PGLD to standardize the information system taxonomy across the IRS to reduce the complexity of our manual reconciliation efforts.

IMPLEMENTATION DATE: September 30, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity; Associate Chief Information Officer, Enterprise Services

Attachment

Audit# 202320016, The IRS is Not Collecting or Protecting Access to All Audit Trail Data

RECOMMENDATION 4: The Chief Information Officer should ensure that the Next Generation ESAT program periodically validates receipt of required audit trail data from all source systems.

CORRECTIVE ACTION 4: We agree with this recommendation. We will document receipt of audit trail data from all source systems.

IMPLEMENTATION DATE: December 29, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

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

CORRECTIVE ACTION 5: We agree with this recommendation. We will automate the disablement of inactive user accounts in accordance with the IRM policies and procedures. This will move us from a manual, cyclical process to an automated real-time process.

IMPLEMENTATION DATE: December 29, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

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.

CORRECTIVE ACTION 6: We agree with this recommendation. We 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.

IMPLEMENTATION DATE: December 29, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Application	An information technology component of a system that uses information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
As-Built Architecture	The authoritative source of the IRS's information technology and business environments. It documents the production environment of IRS systems, infrastructure, technology platforms, *etc*.
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to results.
Data Repository	A database and analytics tool used to analyze the streams of machine data generated by information technology systems and technology infrastructure.
Event	Any action that happens on a computer system. Examples include logging in to a system, executing a program, and opening a file.
Event Forwarding	Allows administrators to obtain events from remote computers, also called source computers or forwarding computers, and store them on a central server known as the collector computer. Agencies shall forward all required logging data, in near real-time, and on an automated basis.
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.
Internal Revenue Manual	The 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.
Legacy	Outdated computer systems, programming languages, or application software that are used instead of more modern alternatives.
Log	A file containing data about an event that occurred in an application or operating system.
Mapping	An operation that associates each element of a given set with one or more elements of a second set.
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.

Term	Definition
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.
Taxonomy	A scheme of classification.
Terabyte	A unit of digital data equal to about 1 trillion bytes.

Appendix V

Abbreviations

ESAT	Enterprise Security Audit Trails
FISMA	Federal Information Security Modernization Act of 2014
FTI	Federal Tax Information
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OMB	Office of Management and Budget
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information

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.