



*Audit Trails Did Not Comply With Standards
or Fully Support Investigations of
Unauthorized Disclosure of Taxpayer Data*

September 20, 2012

Reference Number: 2012-20-099

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

Phone Number | 202-622-6500

E-mail Address | TIGTACommunications@tigta.treas.gov

Website | <http://www.tigta.gov>



HIGHLIGHTS

AUDIT TRAILS DID NOT COMPLY WITH STANDARDS OR FULLY SUPPORT INVESTIGATIONS OF UNAUTHORIZED DISCLOSURE OF TAXPAYER DATA

Highlights

Final Report issued on
September 20, 2012

Highlights of Reference Number: 2012-20-099
to the Internal Revenue Service Chief
Technology Officer.

IMPACT ON TAXPAYERS

Audit trails are a key component of information technology security and contain a record of events occurring on a computer from system and application processes, as well as user activity. The IRS has taken actions to implement an enterprise solution to audit trail weaknesses, but incomplete audit trail data and inconsistent timestamps indicate audit trail processes need improvement. Insufficient audit trail data hinder investigations of unauthorized access (UNAX) to taxpayer information and IRS management's ability to enforce UNAX policies.

WHY TIGTA DID THE AUDIT

UNAX is prohibited by law. This audit was initiated to evaluate the IRS's efforts to implement effective UNAX audit trails for information systems that store and process taxpayer data. This audit is included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The Enterprise Security Audit Trail (ESAT) office has taken several actions to implement an enterprise solution to audit trail weaknesses. However, process improvements are needed to ensure audit trails effectively support UNAX investigations and IRS management's ability to identify noncompliant activity and hold employees accountable for UNAX policies.

Audit Plans, the key planning document to meet IRS goals to comply with audit trail standards,

did not adequately identify all auditable events and related data elements that were required to be captured in the audit trail. Consequently, audit trail logs were missing required data.

TIGTA observed application users while transactions were entered on three IRS applications that send audit trails to the Security Audit and Analysis System, the IRS's audit trail repository system. Multiple audit trail weaknesses were identified as a result of tracing these transactions. The IRS did not adequately validate audit log data that were sent to the Security Audit and Analysis System to ensure that the data necessary to support UNAX investigations are captured. The ESAT office did not conduct tests to determine if actions taken by users on the system correlated to events recorded in the audit trail log or if all required elements were being captured.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the ESAT office improve processes to ensure Audit Plans and resulting audit trails are accurate, complete, and compliant with requirements. In addition, processes to test audit trail data should be improved, and the Audit Plan template should be updated to identify the location of information on audit log testing and stakeholder comments and to show ESAT office approval that testing was sufficient. TIGTA also recommended that timestamp procedures be clarified and made readily available to application owners.

In their response, IRS officials stated they agreed with the recommendation to improve processes to test audit trail data. The IRS partially agreed with three recommendations. The IRS did not agree that validation should be completed before final ESAT office approval of Audit Plans, that Audit Plan templates should be updated to identify the location of information on audit log testing and stakeholder comments, or that guidance on timestamps needs revision, although they will review timestamp procedures.

TIGTA continues to recommend that the IRS formalize a location where test and ESAT validation results can be found, set shorter time frames to implement the proposed changes, postpone closing audit trail specific weaknesses, and revise timestamp procedures.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 20, 2012

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael E. McKenney

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data (Audit # 201220004)

This report presents the results of our review of the Internal Revenue Service's efforts to implement effective unauthorized access audit trails for information systems that store and process taxpayer data. This audit is included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Table of Contents

Background	Page 1
Results of Review	Page 4
The Enterprise Security Audit Trail Office Has Taken Actions to Implement an Enterprise Solution to Audit Trail Weaknesses	Page 4
Process Improvements Are Needed to Ensure Audit Trails Effectively Support Unauthorized Access Investigations.....	Page 5
<u>Recommendation 1:</u>	Page 10
<u>Recommendations 2 and 3:</u>	Page 11
<u>Recommendation 4:</u>	Page 12
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 13
Appendix II – Major Contributors to This Report	Page 15
Appendix III – Report Distribution List	Page 16
Appendix IV – Descriptions of Applications.....	Page 17
Appendix V – Management’s Response to the Draft Report	Page 18



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Abbreviations

AMS	Account Management Services
ESAT	Enterprise Security Audit Trail
IRS	Internal Revenue Service
MeF	Modernized e-File
SAAS	Security Audit and Analysis System
TDS	Transcript Delivery System
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Background

The Internal Revenue Service (IRS) relies extensively on computer systems to carry out the responsibilities of administering the Nation's tax laws, including processing Federal tax returns and collecting Federal taxes. IRS computer systems process hundreds of millions of tax and information returns and contain tax information for more than 100 million taxpayers. Because of the sensitivity of these data, the IRS must maintain effective information security controls over its systems to protect financial and taxpayer information from inadvertent or deliberate misuse, improper disclosure, or destruction.

Audit trails are a key component of effective information technology security. Audit trails contain a record of events occurring on a computer from system and application processes,¹ as well as user activity. In essence, audit trails should provide information as to what events occurred, when the events occurred, and who (or what) caused the events. This information can allow an organization to reconstruct events, monitor compliance with security policies, identify malicious activity or intrusion, and analyze user and system activity. Maintaining sufficient audit trails is critical to establishing accountability, particularly over individual users and their activities.

The National Institute of Standards and Technology, the Department of the Treasury, and the IRS's policies and procedures contain requirements for the capture, storage, transmission, review, and retention of audit trails. These policies and procedures require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected on enterprise-computing assets.

Maintaining sufficient audit trails of user activity on computer systems is a critical component of information security.

Due to the sensitive nature of tax return information, Internal Revenue Code Section (§) 6103² and the Taxpayer Browsing Protection Act of 1997³ require the IRS to detect and monitor the unauthorized access (UNAX) and disclosure of taxpayer records. The willful unauthorized access or inspection of taxpayer records is a crime punishable upon conviction by fines, prison terms, and termination of employment.

The implementation of audit trail solutions has been a challenge for the IRS. In 1997, the IRS identified computer security as a material weakness under the Federal Managers' Financial

¹ A system is a set of interdependent computer components that may include software, hardware, and processes. An application is a component of a system and is designed to help the user perform specific tasks, such as accounting functions or word processing.

² Internal Revenue Code § 6103 restricts the disclosure of tax returns and return information.

³ Pub. L. No.105-35, 26 U.S.C. §§ 7213, 7213A, 7431.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Integrity Act of 1982.⁴ The Federal Managers' Financial Integrity Act requires that each agency conduct annual evaluations of its systems of internal accounting and administrative controls, and submit an annual assurance statement on the status of the agency's system of management controls. As part of the evaluations, agency managers identify control areas that can be considered material weaknesses.⁵ The IRS's computer security material weakness included audit trails as one of its nine subsections.⁶ Audit trails were included as part of the computer security material weakness because the IRS was not effectively monitoring key networks and systems to identify unauthorized activities and inappropriate system configurations.

The IRS established the Enterprise Security Audit Trail (ESAT) Project Management Office (hereafter referred to as the ESAT office) within its Cybersecurity organization in March 2010. The ESAT office's mission is to resolve the IRS's audit trail material weakness by managing all enterprise audit initiatives and overseeing the deployment of various audit trail solutions that meet the required standards.⁷ The IRS decided that audit trails for systems that store or process taxpayer data should be sent to the Security Audit and Analysis System (SAAS), where they could be accessed by those responsible for reviewing questionable activities and investigating potential UNAX violations. The SAAS is the audit trail repository for both projects in development and existing production applications when taxpayer data are accessed.

Despite the IRS's requirement that employees complete UNAX awareness training annually, which emphasizes that accessing taxpayer information without a business justification is a security violation, the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations investigates an average of nearly 400 UNAX violations each year. The TIGTA Office of Investigations uses various sources of information to detect potential unauthorized accesses to tax return information including audit trails generated by the Integrated Data Retrieval System, the Modernized e-File (MeF) system, the Transcript Delivery System (TDS), and the Account Management Services (AMS).⁸

⁴ 31 U.S.C. §§ 1105, 1113, 3512 (2000).

⁵ The Department of the Treasury has defined a material weakness as, "shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports."

⁶ The nine subsections of the computer security material weakness are: 1) network access controls, 2) system and application access controls, 3) system software configuration, 4) security roles and responsibilities, 5) separation of duties, 6) contingency planning, 7) audit trails, 8) security-related training, and 9) certification and accreditation. The IRS has completed actions to remediate the separation of duties, training, and certification and accreditation subsections.

⁷ Similar functions were carried out by a predecessor organization called the Computer Security Audit Trail organization established in 2008.

⁸ The Integrated Data Retrieval System is an IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records. See Appendix IV for a description of the MeF system, the TDS, and the AMS. These applications send audit trails to the SAAS, but only Integrated Data Retrieval System audit trails are complete in the SAAS.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

In addition, IRS security specialists review daily SAAS audit log reports for suspicious or unauthorized activities. If noncompliant activity is found, IRS managers are required to initiate disciplinary actions. Making sure that systems capture required events accurately and completely in the SAAS is critical to the resolution of the audit trail material weakness, adequate UNAX detection efforts, and IRS management's ability to enforce UNAX policies.

This review was performed at the Modernization and Information Technology Services⁹ organization Office of Cybersecurity in New Carrollton, Maryland, during the period September 2011 through May 2012. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

⁹ On July 1, 2012, the Modernization and Information Technology Services organization changed its name to the Information Technology organization.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Results of Review

The ESAT office has taken actions to implement the SAAS as the enterprise solution to address audit trail weaknesses. However, its actions did not result in a process that was effective in supporting UNAX investigations. As a result, UNAX investigations may be difficult or impossible to accomplish using the SAAS, the stated enterprise solution. Without the audit data needed to complete UNAX investigations, IRS management may be unable to identify or substantiate noncompliant activity, or hold employees accountable to UNAX policies. Additionally, the IRS should not rely on the SAAS to address the computer security material weakness related to audit trails until improvements have been made to better capture key audit trail data.

The Enterprise Security Audit Trail Office Has Taken Actions to Implement an Enterprise Solution to Audit Trail Weaknesses

The ESAT office has been instrumental in helping application owners produce plans to implement audit trail policies and procedures. It has developed an Audit Plan template to ensure that policies and procedures are considered when decisions are made as to which information should be captured for audit trails. It also has acted as a facilitator and resource to application owners as they develop the Audit Plans. In addition, the ESAT office has been receptive to stakeholder input from the TIGTA Office of Investigations about potential changes that should be made to the process. For example, based on TIGTA Office of Investigations' input, the ESAT office added requirements to the Internal Revenue Manual¹⁰ that improved audit trails, enhanced educational efforts to application owners on what constitutes auditable events, and more frequently sought stakeholder input during Audit Plan formation that resulted in better plans.

Audit Plans, which contain critical audit trail details, such as which events and data elements are used by an application, are the most important document to ensure that audit trail standards are met and all the required information is captured. IRS policy states that every interaction with taxpayer information through an application is an auditable event. Application owners are directed to document the following audit trail information in their Audit Plans.

- What events occurred (*e.g.*, add, delete, modify, or research).
- When the events occurred (*i.e.*, timestamp).
- Who (or what) caused the events.

¹⁰ Internal Revenue Manual 10.8.3, *Information Technology Security, Audit Logging Security Standards*.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

- Success or failure of the transaction.
- Information related to the taxpayer's identity, tax form type, and tax period.
- Any supplemental information on specific individuals or transactions requiring additional oversight.

The Audit Plan is customized to each individual application and parallels audit trail guidance from the National Institute of Standards and Technology in *Recommended Security Controls for Federal Information Systems and Organizations* (Special Publication 800-53). Once completed, the ESAT office must approve and sign off on each application's Audit Plan.

The IRS's goal is that all applications in which taxpayer information is accessed, whether the application is in development or in production, will eventually send audit trails to the SAAS. The ESAT office's tracking sheet shows that it identified 380 applications that could potentially contain taxpayer information and therefore be required to send audit trails to the SAAS. Because some of those 380 systems will be retired or are subsystems, the ESAT office estimates that currently 339 applications potentially require an Audit Plan. However, the ESAT office has not evaluated whether these applications actually contain taxpayer information and therefore would need to send audit trails to the SAAS. The ESAT office did not know of any other source of information at the IRS that could provide this determination for these applications. In general, the ESAT office has been prioritizing the completion of Audit Plans for new applications in development and applications included in Federal Information Security Management Act reports. ESAT officials advised us that they have reviewed and approved 83 application Audit Plans. As of March 2012, the SAAS contained audit trail data from 20 applications.

The ESAT office has taken additional actions to address SAAS deficiencies and to promote acceptable UNAX monitoring. For example, it has recently overseen the addition of three new data fields in the SAAS to improve compliance with audit trail standards and ensure the capture of required audit trail data elements.

Despite these accomplishments, we identified several factors that have hindered the ESAT office's further progress in making the SAAS an effective enterprise audit trail solution for UNAX monitoring and in addressing and resolving the audit trail material weakness.

Process Improvements Are Needed to Ensure Audit Trails Effectively Support Unauthorized Access Investigations

Audit Plans, the key planning document to meet the IRS's goals to comply with audit trail standards, did not adequately identify all auditable events and related data elements that were required to be captured in the audit trail. Consequently, SAAS data did not include key events and data elements in the audit trail. The SAAS data also were not always captured in a usable format, and the timestamp was not consistent. The data were generally collected as anticipated in the Audit Plans, but the Audit Plans did not adequately describe all of the data that should



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

have been collected. These issues may compromise investigations and the IRS's ability to eventually close the audit trail subsection of the computer security material weakness.

Audit plans did not include all events and data elements

We selected a judgmental sample¹¹ of three applications to review for accuracy and completeness of the Audit Plans and SAAS data. An important consideration in our selection was whether the applications qualified as meeting the closure criteria for one of the audit trail corrective actions for the computer security material weakness.¹² We selected the following applications: the AMS, the TDS, and the MeF system. These applications collectively process or store taxpayer data on potentially every taxpayer account.

Two of the three Audit Plans we reviewed, although approved by the ESAT office, did not identify all application events that involve access to taxpayer data. For example, the TDS used the same event description for every transaction that occurred. The AMS used four different event descriptions, but they were not sufficient to identify exactly which document had been accessed or whether the document was added, deleted, modified, or used for research (viewed). The MeF system Audit Plan identified the key events and had a good description for them.

Similarly, the Audit Plans did not specify how all the required data elements would be collected for each event. For example, IRS policies require capturing the type of tax form and the tax period for each event when taxpayer information is accessed; however, the Audit Plans did not specifically address how these data elements should be captured. A complicating factor was that the SAAS was unable to capture these required data elements as separate fields until September 2011. However, they could have been recorded in a large "variable" field that was available to all applications.

The description of auditable events in Internal Revenue Manual 10.8.3 and the Audit Plan template is unclear. The manual states that when a taxpayer record has been added, deleted, modified, or researched, that event shall be captured and recorded. However, neither the manual nor the Audit Plan template provide sufficient details on how to translate application transactions to audit trail events or to ensure sufficient events are recorded for each type of transaction.

ESAT officials stated that although they are responsible for oversight of the Audit Plan process and the SAAS, they are only facilitators and do not possess the depth of technical knowledge

¹¹ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

¹² The audit trail subsection of the computer material weakness contains 10 corrective actions, one of which required the implementation of an application monitoring capability for at least four applications. In January 2011, the System Security and Privacy Executive Steering Committee approved closure of this corrective action based on the ESAT office's determination that the SAAS was in continuous receipt of security logs for 16 applications, that the logs were retained in accordance with Internal Revenue Manual 10.8.3, that Cybersecurity organization analysts were dedicated on a per application basis to exercise log analysis, and that the analysts were able to generate appropriate and useful reports against activities from these applications.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

necessary to assist application owners in the detailed preparation of the Audit Plans. Instead, the ESAT office relies on the application owner's resources and expertise to complete the Audit Plan. However, the ESAT office has signatory authority and oversight responsibility for the Audit Plans. If Audit Plans do not document all the information necessary to ensure that the required who, what, when, and where is logged, the IRS has no assurance that the SAAS audit trail data will sufficiently log these details.

The ESAT office did not ensure sufficient testing of audit trail data to validate its accuracy and completeness

The ESAT Audit Plan process does not include essential steps to adequately validate audit log data to ensure the SAAS is capturing the required elements necessary to support UNAX investigations. In addition, the results from the limited testing that is performed are not recorded as part of the Audit Plan.

ESAT officials informed us that they do conduct various validity checks on the data loaded into the SAAS, but they do not verify that audit trails capture all that is required. The ESAT office's testing of data sent to the SAAS is limited to only confirming receipt of data, conducting character validity checks for each SAAS data field, and determining that the reporting feature within the SAAS is functioning properly. It does not conduct transaction-based tests on the data in the SAAS to ensure it is accurate, complete, and meets requirements. Specifically, the ESAT office does not conduct tests to determine whether actions taken by users on the system correlate to events recorded in the SAAS audit trail, or that all required elements are being captured in SAAS.

In December 2011, we observed various transactions performed by application users on our three sample applications and analyzed the resulting audit trail data sent to the SAAS. None of the three applications sent sufficient audit trail data to the SAAS that would allow for easily reconstructing events. The events and data elements in the SAAS generally paralleled those described in the Audit Plan and, consequently, the same issues were present; key events and data elements were not captured. We also identified additional deficiencies through our transaction testing. Figure 1 provides details of the audit trail weaknesses identified during our review. Improvements made to the AMS and the TDS subsequent to our testing are described in footnotes 13 and 14.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Figure 1: Audit Trail Weaknesses of Sampled Applications

Audit Weakness	AMS	TDS	MeF System
No one-to-one correlation exists between transactions accessing a tax record and events recorded in the SAAS. For example, two returns from different years could be accessed, but only one record would appear in the SAAS.	√	√	
Required data elements were missing in the SAAS, such as type of tax form, tax period, and the success or failure of the transaction.	√	√	√
Additional data elements needed for UNAX investigations were missing in the SAAS, such as the type of taxpayer (individual or business).	√	√	√
Events recorded in the SAAS were not sufficiently descriptive to determine what type of taxpayer information had been accessed.	√	√	
Variable field data in SAAS audit trails did not follow a standard format and were mostly not relevant for investigative purposes.	√	√	√
The timestamp was not correctly captured or was not synchronized.	√		√
The application name was not captured in the SAAS.	√		
Accesses made through the AMS to information in other systems were not in the SAAS.	√		

Source: TIGTA analysis of SAAS audit trails.

In addition to not recording events and data elements that fully reflected the nature of the transactions we observed, we also identified three other deficiencies where some events were not captured as they occurred, variable fields contained long strings of useless information, and timestamps were inconsistent from application to application and may not have been properly synchronized.

¹³ Subsequent to our testing, the AMS was revised so that the AMS name is now captured along with its log entries in the SAAS.

¹⁴ The TDS captured a data element for the success or failure of the transaction, but did not capture two other required data elements. Additionally, TDS staff stated that subsequent to our testing, they made improvements to the SAAS audit trail, including that each transaction is captured separately (we confirmed that now a one-to-one correlation between transactions and SAAS records exists), and the variable field uses a standard format that contains relevant information.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Our testing showed that some events were not captured as they occurred. Specifically, we found no one-to-one correlation between transactions and the events that were recorded in the SAAS. For example, when two returns from different tax years were accessed in the same user session, only one record was written to the SAAS, and it did not capture the tax years. Additionally, the AMS allowed users to access information from other applications, and these accesses were not recorded in the SAAS either by the AMS or the other applications. End users had access to this untracked information even when they did not have approval to access the other applications directly.

The SAAS variable field, which was used to capture any relevant information not already captured in defined fields, contained some information. Prior to implementing separate fields for certain required data elements, such as the type of tax form and the tax period, the variable field could be used to capture that information. Additionally, applications may use the variable field to capture information that might be useful to investigations, such as taxpayer representative contact information or fax numbers. However, most of the information captured was a string of programming code for the transaction or the document. The code sometimes contained no relevant information at all and sometimes contained information that was relevant but unformatted (and thus not usable for investigative purposes). Much of this information was useless and capturing it may strain computer capacity, which the IRS has indicated is an issue for audit trail data. Application owners told us they did this because initially no specific guidance existed on how to put formatted information in the field.

The IRS mandates an authoritative time server be used for the purpose of synchronizing the computer system clocks (used for the event timestamp). Synchronization ensures proper sequencing of transactions recorded in audit trails, which is important in developing reliable and convincing investigation results. However, the IRS policy is vague, and the IRS has been unable to provide detailed procedures regarding how this policy is supposed to be implemented. When asked, IRS personnel could not definitively state how to determine the proper time zone for the timestamp, or what the authoritative time server is for synchronizing system clocks. Consequently, we noted discrepancies in audit event timestamps, which could thwart investigations and law enforcement activities. Until the IRS provides system owners with adequate procedures related to synchronization and timestamps, it cannot ensure that audit trail events will be accurately time stamped and able to support UNAX investigations.

The weaknesses described in and after Figure 1 could have been identified by the IRS if adequate audit log validation and testing had been performed. Our analysis compared detailed records of observed transactions conducted by application users to the audit trails from both the application and the SAAS. For example, through a simple input/output comparison, we found that the SAAS did not contain a record for every transaction that was input at the application level, and that the SAAS record was not always sufficient to determine what document had been viewed and when. Without sufficient testing of audit log data, the IRS cannot confirm that actions performed on a system can be reconstructed in support of a UNAX investigation.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Incomplete audit trail data and inconsistent timestamps hinder investigations and affect the IRS's ability to address the computer security material weakness

The SAAS cannot be a good audit trail enterprise solution as long as it continues to lack events, data elements, and consistent timestamps. Insufficient audit trail data hinder investigations of IRS policy violations, suspicious activity, and unauthorized access to taxpayer information. Employees may be less deterred from engaging in malicious or unauthorized activity if they believe their activities are not being monitored.

Implementing a repeatable process to ensure that applications capture all required audit trail events is also critical to the resolution of the audit trail subsection of the computer security material weakness. The IRS has worked for years to develop an effective way to address this weakness and has made continuous incremental improvements. The IRS developed multiple corrective actions to deal with audit trail weaknesses, one of which related to employing the SAAS to capture and report on audit trail data. The SAAS appeared to be accomplishing this corrective action as the IRS had framed it and, consequently, IRS management deemed this corrective action ready for closure. However, until a repeatable process is in place to ensure the audit trail data in the SAAS are complete and accurate, the IRS should not rely on SAAS data to support closure of the material weakness.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Ensure the ESAT office improves processes to ensure Audit Plans are accurate, complete, and compliant with requirements prior to signing the Audit Plans; specifically, that meaningful events, required data elements, and descriptive variable information are captured in the SAAS audit trails for all applications. The ESAT office should facilitate development of application Audit Plans with collaboration between the application owner who prepares the Audit Plan and stakeholders of the audit trails, including the Cybersecurity organization and the TIGTA Office of Investigations. Comments and concerns of the stakeholders with respect to the Audit Plans should be documented and resolved.

Management's Response: The IRS partially agreed with this recommendation. The ESAT office will ensure that Audit Plans are accurate, complete, and compliant with Internal Revenue Manual 10.8.3 requirements prior to signing. The ESAT office will facilitate the development of application Audit Plans in collaboration with the application owner and stakeholders, including Cybersecurity and the TIGTA Office of Investigations. Stakeholder comments and concerns about the Audit Plans will be documented and resolved. The capture of meaningful events, required data elements, and descriptive variable information for all applications will be improved in the SAAS audit trails as set forth in the Audit Plans. However, the IRS disagreed that validation should be completed prior to signing the Audit Plans.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Office of Audit Comment: We have concerns with the implementation date of this corrective action by November 1, 2016, more than four years after the issuance of this report. Without the collaboration of the stakeholders and improved processes to document and resolve their comments and concerns while Audit Plans are being developed, the IRS will have no assurance that the accuracy and completeness of Audit Plans will improve in order for the compliance of the resulting audit trails to improve. Therefore, we recommend immediate implementation of this corrective action. We are also in agreement that the ESAT office's validation of audit trails would occur subsequent to its signing of the Audit Plan, and did not intend otherwise in Recommendation 1.

Recommendation 2: Ensure the ESAT office improves processes to test audit trail data; specifically, to validate that details from transactions entered into the application are complete and timestamps are consistent in the SAAS, not just that data are being successfully transmitted to the SAAS. Validation of audit trails should also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Comments of the stakeholders with respect to audit trail testing should be documented.

Management's Response: The IRS agreed with this recommendation. The ESAT office will improve processes to test audit trail data to validate that details from transactions entered into the application are complete and timestamps are consistent in the SAAS, not just that data are being successfully transmitted to the SAAS. Validation of audit trails will also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Stakeholder comments and concerns about the audit trails testing will be documented.

Recommendation 3: Ensure the ESAT office updates the Audit Plan template to include: 1) a statement that audit trails must allow for subsequent forensic reconstruction and review of employee user-initiated actions by identifying the element of account information (*i.e.*, document, form, case file, or narrative) and which of the four actions (added, deleted, modified, or researched) was taken on the account; 2) information about where audit trail testing results and stakeholder comments regarding the Audit Plan development can be found; and 3) a second ESAT approval on the Audit Plan to verify that sufficient testing of audit trails was completed.

Management's Response: The IRS partially agreed with this recommendation. The information requested in part 1 of this recommendation is already included in the Audit Plan template in accordance with Internal Revenue Manual 10.8.3. The IRS agrees the ESAT office will improve processes to test audit trail data to validate that details from transactions entered into the application are complete as specified in the Audit Plan. Validation of audit trails will also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Stakeholder comments and concerns about audit trail testing will be documented and retained. The



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

IRS disagreed that the Audit Plan template should be updated to include information about where stakeholder comments regarding the Audit Plan development and the audit trail testing results can be found. The IRS also disagreed that a second ESAT approval should be conducted for the Audit Plan to indicate testing was completed. However, any changes to the Audit Plans determined as necessary from test results analysis will be addressed immediately.

Office of Audit Comment: The IRS disagreed to update the Audit Plan template to include information regarding audit trail testing and proposed no alternative solution or location. We continue to recommend that the ESAT office's improved audit trail testing processes formalize a location where test results and the ESAT office's validation of the audit trail data can be found. Currently, the IRS is using ESAT-approved Audit Plans to close audit trail weaknesses at the application level and at the IRS organizational level. However, ESAT-approved Audit Plans provide no assurance that the audit trails are compliant with requirements. Those who test audit trail controls at the application and organization levels during security control assessments or annual testing of controls should be instructed to base the status of the audit trail controls on ESAT-validated audit trails, not on ESAT-approved Audit Plans. We also have concerns that the IRS has set the implementation date for its improvement of audit trail testing processes to be November 1, 2016, and believe a shorter time frame should be set. Until processes are in place for proper testing and the ESAT office's validation of audit trails, audit trail-specific weaknesses at the application or organizational level should not be closed.

Recommendation 4: Revise policies and procedures to ensure timestamp guidance is clear and readily available to application owners. Guidance should include which devices serve as authoritative time servers for synchronization, how to configure local systems to synchronize with authoritative time servers, and where to locate assistance if needed.

Management's Response: The IRS partially agreed with this recommendation. Guidance that describes which devices serve as authoritative time servers and how local systems are configured to align with those servers did exist, but was not readily available for the auditors. The IRS will review existing policies and procedures for timestamps and ensure the guidance is clear and available to all stakeholders.

Office of Audit Comment: We continue to recommend the IRS ensures that its policies and procedures related to timestamp guidance be revised, not just reviewed with no assurance that they will be revised. The IRS needs to adequately document or log the actual time zone in the Audit Plan or within the audit trail. The current process leaves time zones up to interpretation, which can be detrimental to any administrative or criminal investigation, and resulting adjudications of potential UNAX cases.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's efforts to implement effective UNAX audit trails for information systems that store and process taxpayer data. To accomplish our objective, we:

- I. Determined whether the IRS has an effective process to comply with application audit trail requirements in the preparation of Audit Plans and sending audit trail information to the SAAS.
 - A. Identified and reviewed policies, procedures, and guidelines related to the audit trail process.
 - B. Interviewed the Cybersecurity organization's ESAT Project Management Office (hereafter referred to as the ESAT Office) personnel and other Cybersecurity organization personnel to document and assess the procedures for preparing and approving Audit Plans, and verifying the completeness and accuracy of data sent to the SAAS.
 - C. Evaluated the IRS's progress towards implementing adequate audit trails for its population of applications that contain taxpayer data.
- II. Determined if either the application project office or the application owner has completed and approved an Audit Plan in compliance with ESAT office guidance, and the Audit Plan accurately identifies all required auditable events.
 - A. Identified the population of applications in use by the IRS and selected a judgmental sample for further review and testing.
 1. Obtained a list of applications dated July 27, 2011, indicating the TIGTA Office of Investigations' and the ESAT office's priorities.
 2. Selected a judgmental sample of three applications for detailed testing from 199 applications identified by the TIGTA Office of Investigations. Consideration for selection included whether the application processes and stores taxpayer data, has completed an Audit Plan, is sending audit trail information to the SAAS, has been identified to support the closure of the computer security material weakness for audit trails, and is categorized as high priority by the TIGTA Office of Investigations and/or the ESAT office. We selected a judgmental sample due to staff resource constraints, and we did not plan to project our results.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

- B. Obtained and reviewed core record layouts of audit trails and IRS employee training materials to identify transactions that read, write, execute, modify, or delete taxpayer accounts.
 - C. Interviewed front-line employees or managers to ensure application events that read, write, execute, modify, or delete taxpayer data are identified in the Audit Plan.
 - D. Determined whether the Audit Plan accurately addresses all taxpayer transaction capabilities (read, write, execute, modify, delete) as identified in interviews, training records, core record layouts, and variable definitions.
 - E. For issues identified, interviewed appropriate personnel and/or obtained documentation to determine the cause.
- III. Determined whether the applications selected for review capture a complete and accurate audit trail of information necessary to support forensic investigation of transactions involving taxpayer information.
- A. Conducted field observations of different types of transactions being input to the sample applications and recorded the information.
 - B. Obtained application audit trails from the application owner or project office, along with SAAS audit trails, to verify that field observation transactions were complete and accurately captured in the audit trails.
 - 1. Verified that the elements for each of the transactions executed during field observations matched the audit trail transaction elements.
 - 2. For those transactions not executed during field observations, verified through review of the audit trails that they were being captured. If additional transactions that read, write, execute, modify, or delete taxpayer information were not identified in the sample audit trail extracts, we contacted the application owner or project office to provide supporting evidence that these transactions were being captured in audit trails.

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 the following internal controls were relevant to our audit objective: IRS policies, procedures, and practices for capturing, storing, transmitting, reviewing, and retaining audit trails. We evaluated these controls by reviewing IRS policy and procedure documents, interviewing IRS personnel, and observing various transactions performed by application users on our three sample applications and analyzing the resulting audit trail data.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)

Kent Sagara, Director

Jody Kitazono, Audit Manager

Myron L. Gulley, Senior Auditor

Mary Jankowski, Senior Auditor

Louis Lee, Senior Auditor

Sam Mettauer, Senior Auditor



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Appendix IV

Descriptions of Applications

Application	Description
Account Management Services	The purpose of the AMS is to provide an integrated approach to view, access, update, and manage taxpayer accounts by providing IRS employees with the tools necessary to access information quickly and accurately in response to complex customer inquiries and to update taxpayer accounts on demand. Functionality includes inventory management; next case delivery; nationwide history and follow-ups; correspondence received from taxpayers concerning lost, stolen, destroyed, or returned refunds; immediate print capabilities to fax to taxpayers; and generation of electronic referrals. As of March 2012, the AMS had processed more than five million transactions since it was implemented in September 2009.
Modernized e-File	The MeF system runs on a modernized, Internet-based electronic file platform. Its purpose is to provide a single method for filing all business and individual tax returns, forms, and schedules via the Internet. The MeF system provides real-time processing of tax returns that improves error detection, standardizes business rules, and expedites acknowledgments. MeF system volume has been increasing due to the phasing in of its components. For Calendar Year 2012 (as of March), the MeF system had accepted more than 59 million individual and business returns (out of about 83 million returns submitted).
Transcript Delivery System	The purpose of the TDS is to provide self-service for return and account information requests by external customers. The TDS automates the validation, processing, and delivery of taxpayer information to the authorized third-party user. TDS transactions include self-service electronic communication, where the user can request and receive a transcript product interactively. The user will have the ability to specify an information delivery method by systematic responses, automatic fax, or postal mail. As of March 2012, the TDS had processed more than 144 million transactions since it was implemented.

Source: TIGTA, Ref. No. 2008-20-053, The Account Management Services Project Is Meeting Its Development Goals pp. 1, 8, 52 (Mar. 2008); TIGTA, Ref. No. 2011-40-131, Low Participation and Tax Return Volumes Continue to Hinder the Transition of Individual Income Tax Returns to the Modernized e-File System p. 1 (Sept. 2011); the IRS As-Built Architecture website; and the March 2012 Modernization and Information Technology Services Business Value Chart.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

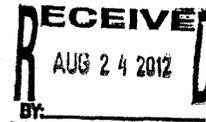
Appendix V

Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



AUG 24 2012

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report – Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data(Audit # 201220004)(i-trak #2012-34307

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. We appreciate the recognition that the Internal Revenue Service has taken additional steps to address Security Audit and Analysis System deficiencies and to promote acceptable UNAX monitoring.

The IRS is committed to continuously improving the security of our information technology systems and implementing effective unauthorized access audit trails for information systems that store and process taxpayer data. The attachment to this memo details our planned corrective actions to implement the audit report's recommendations.

If you have any questions, please contact me at (202) 622-6800 or Brian Buckley, Director of Risk Management, at (202) 283-4613.

Attachment



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Attachment

Draft Audit Report – Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data (Audit # 201220024)
(e-trak #2012-34307)

RECOMMENDATION #1: The Chief Technology Officer should ensure the ESAT office improves processes to ensure audit plans are accurate, complete, and compliant with requirements prior to signing the audit plans; specifically, that meaningful events, required data elements, and descriptive variable information are captured in the SAAS audit trails for all applications. The ESAT office should facilitate development of application audit plans with collaboration between the application owner who prepares the audit plan and stakeholders of the audit trails, including the Cybersecurity organization and the TIGTA Office of Investigations. Comments and concerns of the stakeholders with respect to the audit plans should be documented and resolved.

CORRECTIVE ACTION #1: We agree with this recommendation in part. The Enterprise Security Audit Trail Project Office will ensure that audit plans are accurate, complete, and compliant with requirements (as specified in IRM 10.8.3) prior to signing. The ESAT office also will facilitate the development of application audit plans. This will be done in collaboration with the application owner who will prepare the audit plans and stakeholders of the audit trails, including the Cybersecurity organization and the TIGTA Office of Investigations. Stakeholder comments and concerns about the audit plans will be documented and resolved.

The capture of meaningful events, required data elements, and descriptive variable information for all applications will be improved in the SAAS audit trails as set forth in the audit plans. We disagree that this validation will be completed prior to signing the audit plans. Validation is part of the testing stage of the application life cycle, and is the time during which the test results will be documented. However, any necessary changes to the audit plans determined as necessary from analysis of the test results will be addressed immediately.

IMPLEMENTATION DATE: November 1, 2016

RESPONSIBLE OFFICIAL: Associated Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.



*Audit Trails Did Not Comply With Standards or Fully Support
Investigations of Unauthorized Disclosure of Taxpayer Data*

Attachment

Draft Audit Report – Audit Trails Did Not Comply With Standards or Fully Support
Investigations of Unauthorized Disclosure of Taxpayer Data (Audit # 201220024)
(e-trak #2012-34307)

RECOMMENDATION #2: The Chief Technology Officer should ensure the ESAT office improves processes to test audit trail data; specifically, to validate that details from transactions entered into the application are complete and timestamps are consistent in the SAAS, not just that data are being successfully transmitted to the SAAS. Validation of audit trails should also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Comments of the stakeholders with respect to audit trails testing should be documented.

CORRECTIVE ACTION #2: We agree with this recommendation. The ESAT PMO will improve processes to test audit trail data, specifically, to validate that details from transactions entered into the application are complete and timestamps are consistent in the SAAS, not just that data are being successfully transmitted to the SAAS. Validation of audit trails will also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Stakeholder comments and concerns about the audit trails testing will be documented.

IMPLEMENTATION DATE: November 1, 2016

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Attachment

Draft Audit Report – Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data (Audit # 201220024) (e-trak #2012-34307)

RECOMMENDATION #3: The Chief Technology Officer should ensure the ESAT office updates the Audit Plan template to include 1) a statement that audit trails must allow for subsequent forensic reconstruction and review of employee user initiated actions by identifying the element of account information (i.e., document, form, case file or narrative) and which of the four actions (added, deleted, modified, or researched) was taken on the account; 2) information about where audit trail testing results and stakeholder comments regarding the Audit Plan development can be found; and 3) a second ESAT approval on the Audit Plan to verify that sufficient testing of audit trails was completed.

CORRECTIVE ACTION #3: We agree with this recommendation in part. The information requested in Part (1) of this recommendation is already included in the audit plan template in accordance with IRM 10.8.3. We agree the ESAT office will improve processes to test audit trail data: specifically, to validate that details from transactions entered into the application are complete as specified in the audit plan. Validation of audit trails will also be a collaborative effort with stakeholders, including the Cybersecurity organization and the TIGTA Office of Investigations. Stakeholder comments and concerns about audit trail testing will be documented. We disagree that the audit plan template should be updated to include information about where stakeholder comments regarding the audit plan development and the audit trail testing results can be found. However, stakeholder comments during the audit plan development and review will be retained as per standard documentation procedures, along with the final audit plan. We disagree that a second ESAT approval will be conducted for the audit plan to verify that sufficient audit trails testing was completed. However, any changes to the audit plans determined as necessary from test results analysis will be addressed immediately.

IMPLEMENTATION DATE: November 1, 2016

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.



Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data

Attachment

Draft Audit Report – Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data (Audit # 201220024)
(e-trak #2012-34307)

RECOMMENDATION #4: The Chief Technology Officer should revise policies and procedures to ensure timestamp guidance is clear and readily available to applications owners. Guidance should include which devices serve as authoritative time servers for synchronization, how to configure local systems to synchronize with authoritative time servers, and where to locate assistance if needed

CORRECTIVE ACTION #4: We partially agree. Guidance that describe which devices serve as authoritative time servers and how local systems are configured to align with those servers did exist, but was not readily available for the auditors. The IRS will review existing policies and procedures for timestamps and ensure the guidance is clear and available to all, stakeholders.

IMPLEMENTATION DATE: March 1, 2013

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.