Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected

September 17, 2015

Reference Number: 2015-20-088

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

IMPROVEMENTS ARE NEEDED TO ENSURE THAT NEW INFORMATION SYSTEMS DEPLOY WITH COMPLIANT AUDIT TRAILS AND THAT IDENTIFIED DEFICIENCIES ARE TIMELY CORRECTED

Highlights

Final Report issued on September 17, 2015

Highlights of Reference Number: 2015-20-088 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Audit trails are a key component of effective information technology security. Maintaining sufficient audit trails is critical to establishing accountability over users and their actions within information systems. Due to the sensitive nature of tax return data, the IRS is required by law to detect and monitor the unauthorized access and disclosure of taxpayer records. Without sufficient audit trails, the IRS will be unable to identify or substantiate noncompliant activity that puts taxpayer records at risk.

WHY TIGTA DID THE AUDIT

Implementing audit trail solutions has long been a challenge for the IRS. The IRS reported audit trails as an area of material weakness in Fiscal Year 1997 and as a significant deficiency since Fiscal Year 2012. The IRS established an office to coordinate an enterprise solution for resolving its audit trail deficiencies that would include processes for both legacy and newly deployed systems to meet the required standards. This audit was initiated to evaluate the IRS's efforts to implement effective audit trails for new information systems that store and process taxpayer data and to track and correct identified deficiencies in existing audit trails.

WHAT TIGTA FOUND

The IRS continues to make progress in implementing its enterprise solution to address its audit trail deficiencies. However, the IRS needs to strengthen controls in its new systems development and deficiency remediation processes to improve the number and quality of its audit trails.

TIGTA found that not all IRS systems in development in recent years had audit trail requirements adequately assessed prior to deployment. Of the systems for which an audit plan was completed during the development process, most were not transmitting audit trails in accordance with IRS requirements when deployed. Without fully operational audit trails, unauthorized accesses could be made within these systems and may not be detected. In addition, TIGTA found that system owners were not timely entering identified audit trail deficiencies into Plans of Action and Milestones to ensure proper tracking and remediation. As such, the deficiencies could persist indefinitely.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) amend procedures to ensure that systems in development are evaluated for audit trail requirements in a timely manner; 2) ensure that the document which new system owners must complete prior to transmitting audit trails is included as one of the required systems development documents; 3) revise guidance to clearly state system owner responsibility for audit trails, including the requirement for addressing identified audit trail deficiencies in a timely manner; and 4) ensure that appropriate annual testing of audit trail controls is conducted and any identified deficiencies are reported.

The IRS agreed with our recommendations except for the first, to which it partially agreed. IRS management amended procedures to ensure that systems in development are evaluated for audit trail requirements in a timely manner, clarified guidance on the document needed to transmit audit trails, communicated to system owners their responsibility for audit trail controls and deficiencies, and updated its processes to ensure annual testing procedures identify audit trail deficiencies. The IRS also plans to use procedures that will ensure that audit trail deficiencies are timely reported.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 17, 2015

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected (Audit # 201520004)

This report presents the results of our review of the Internal Revenue Service's (IRS) efforts to implement effective audit trails for new information systems that store and process taxpayer data and to track and correct identified deficiencies in existing audit trails. This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CY	Calendar Year
ESAT	Enterprise Security Audit Trail
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SAAS	Security Audit and Analysis System
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized access

Background

Implementing audit trail solutions has long been a challenge for the Internal Revenue Service (IRS). The IRS reported audit trails as an area of material weakness in Fiscal Year 1997[1] and as a significant deficiency since Fiscal Year 2012. 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[2] as well as from 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 IRS reported audit trails as an area of material weakness in Fiscal Year 1997 and as a significant deficiency since Fiscal Year 2012. Maintaining sufficient audit trails is critical to establishing accountability.

National Institute of Standards and Technology, Department of the Treasury, and IRS policies contain requirements for the capture, storage, transmission, review, and retention of audit trails. These policies require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity occurs or is suspected on IRS systems. Due to the sensitive nature of tax return information, Internal Revenue Code Section (§) 6103[3] and the Taxpayer Browsing Protection Act of 1997[4] 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.

To coordinate an enterprise solution for the audit trail weaknesses, the IRS established the Enterprise Security Audit Trail Project Management Office (ESAT office) within its

[1] 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." A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit the attention of those charged with governance.
[2] 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.
[3] Internal Revenue Code § 6103 restricts the disclosure of tax returns and return information.
[4] U.S.C. §§ 7213, 7213A, 7431.

Cybersecurity organization in March 2010.[5] The ESAT office's mission is to resolve the IRS's systemic audit trail issues by managing all enterprise audit initiatives and overseeing the deployment of various audit trail solutions that meet the required standards for legacy and newly deployed systems.

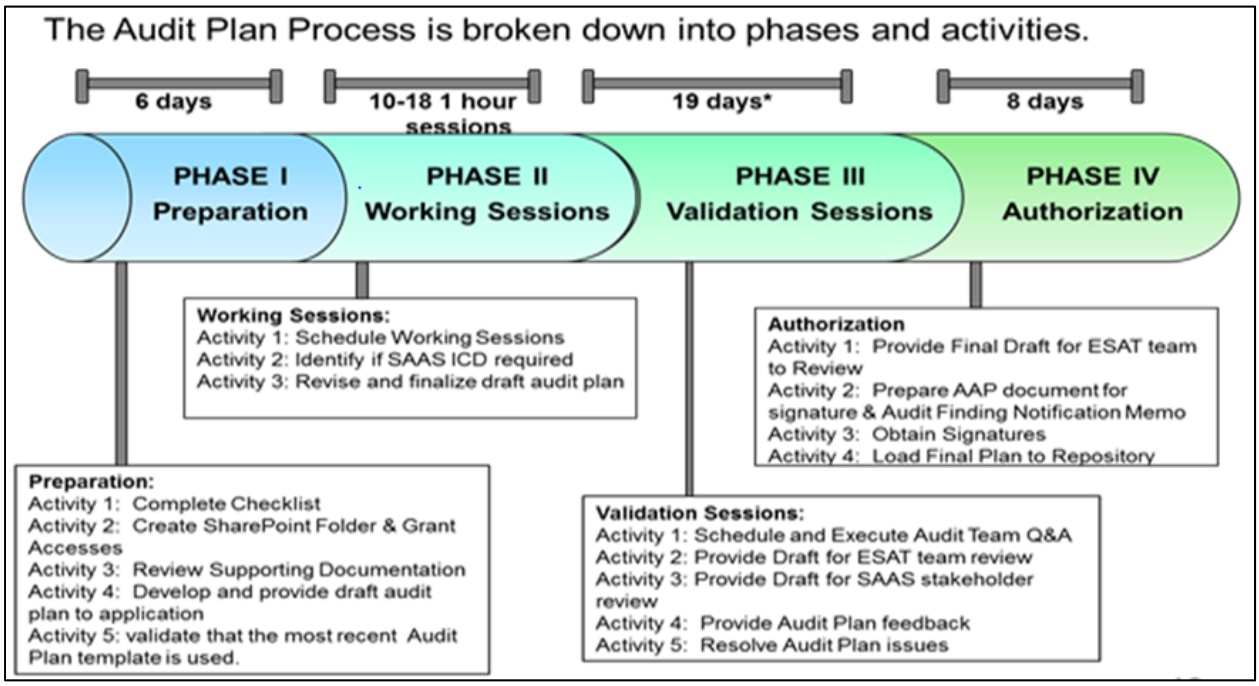
The ESAT office designated the Security Audit and Analysis System (SAAS) as the IRS's enterprise solution to collect audit trails from systems that store or process taxpayer information. SAAS data can be accessed by those responsible for reviewing questionable activities and investigating potential UNAX violations. Recently, the Office of Cybersecurity decided to also send audit trails to the SAAS for systems that do not store or process taxpayer information but do process other types of sensitive information. In addition to its responsibilities related to the SAAS, the ESAT office also manages another system, ArcSight, to capture access data on IRS infrastructure systems, databases, web services, and other components.

A completed audit plan is a key first step in the goal of having usable audit trails. Audit plans provide the framework that describes what type of audit trail data will be captured and how the data interface with other systems. However, the audit plan is just a plan, and having a completed audit plan does not mean the audit trails are being captured as intended. Applications need to take additional steps to have usable audit trails, including developing and implementing an interface control document and testing and successfully transmitting the audit trail data to the SAAS. In addition, subsequent steps to review and ensure that the data are usable are also part of the end goal.

As shown in Figure 1, the IRS has developed a high-level summary chart explaining the four phases and related activities to complete an audit plan.

[5] Similar functions were carried out by a predecessor organization called the Computer Security Audit Trail organization established in Calendar Year 2008.

Figure 1: Application Audit Plan Process Summary



Source: Quarterly ESAT Application Stakeholder Training/Information Technology Cybersecurity.

In a previous report issued in Fiscal Year 2012,[6] the Treasury Inspector General for Tax Administration (TIGTA) found that, although the IRS had taken several actions to implement an enterprise solution to audit trail weaknesses, process improvements were needed. Specifically, audit plans did not adequately identify all auditable events and related data elements that were required to be captured in the audit trail. Consequently, audit trails were missing required data. We also found that, even if audit plans were sufficient, the IRS did not adequately validate audit trails once they were sent to the SAAS to ensure that the data necessary to support UNAX investigations were captured.

Despite the IRS's efforts to educate employees about UNAX, violations do occur. TIGTA's Office of Investigations investigates an average of nearly 400 UNAX violations each year. Even so, the Office of Investigations has expressed concerns to IRS management with the large number of applications not yet sending audit trails to the SAAS, which creates a UNAX detection gap. The Office of Investigations has informed IRS management that the majority of the 83 applications that the Office of Investigations has determined to be subject to UNAX risk do not yet transmit audit trails to the SAAS. At the time of this audit, the Office of

[6] Treasury Inspector General for Tax Administration, Ref. No. 2012-20-099, *Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data* (Sept. 2012).

Investigations had evaluated 10 of 32 unique audit trails that are being sent to the SAAS and determined that only four of the 10 were usable for UNAX investigations.

This review was performed at the IRS Information Technology organization offices at the New Carrollton Federal Building in Lanham, Maryland. We obtained information from management and personnel in the Information Technology's Applications Development and Cybersecurity organizations and the Small Business/Self-Employed and Wage and Investment Division offices in Lanham, Maryland, and Washington, D.C., during the period November 2014 through June 2015. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Several Actions Have Been Taken to Address Systemic Audit Trail Issues

The ESAT office continues to make progress in implementing the IRS's enterprise solution to address audit trail weaknesses related to UNAX. Noteworthy efforts include taking a strategic management approach and developing procedural changes to better highlight audit trail weaknesses to system owners. In addition, the ESAT office has taken several actions to address issues since our prior report, such as:

- Developing a strategic plan to address the enterprise audit trail weakness.
- Initiating a memorandum process to system owners to highlight system deficiencies identified during the audit plan process.
- Addressing some of the guidance issues identified in the prior TIGTA report.
- Assisting system owners in completing audit plans (22[7] signed completed audit plans in Calendar Year (CY) 2013 and eight in CY 2014).

The ESAT office developed a strategic plan, entitled the *Audit Solution Implementation Process*, to correct the IRS's enterprise audit trail deficiencies and to help close the UNAX detection gap. Among other information, the *Automated Solution Implementation Process* describes factors for prioritizing application audit plans, approaches to meeting the SAAS's capacity needs, improvements to be made to the SAAS over time, a description of steps to produce a functional audit trail, cost estimates to develop required documents including the audit plan and interface control document, and key metrics related to audit trails that will be captured. The *Automated Solution Implementation Process* states that the UNAX detection gap due to audit trail weaknesses should be significantly reduced by CY 2021, with 50 percent of the applications that process taxpayer data sending audit trails to the SAAS by then. However, the *Automated Solution Implementation Process* also states that the goal of having end-to-end auditing will not be fully achieved until CY 2027. Until such time, IRS management will continue to lack the ability to fully monitor for UNAX violations, other employee misconduct, or criminal activity occurring in systems that do not transmit complete audit trails to the SAAS enterprise audit trail repository.

In May 2014, the ESAT office started issuing application owners an audit notification memorandum that detailed deficiencies identified while developing the audit plan and interface

[7] One audit plan covered three applications, for a total of 24 applications covered by 22 audit plans.

control document and that explained application owner responsibilities to correct the deficiencies. Prior to the memorandum process, the deficiencies had been identified only in the audit plan. While issuing an audit notification memorandum is a positive step to put application owners on notice about the actions they need to take to correct deficiencies, the application owners have not always been responsive, which will be discussed later in this report.

The ESAT office also took steps to address issues identified in our prior report. The ESAT office modified its audit plan guidance, which will help improve the reliability and quality of SAAS data. Compared to the 2012 audit plan template, the current audit plan template contains more information on the elements that should be collected when taxpayer information is involved, as TIGTA previously recommended. Out of the nine audit plans completed in CY 2014 or early CY 2015 that we reviewed, only one had not adequately addressed all of the required elements, which is an improvement over prior years. Additionally, the interface control document template now contains a page where responsible parties sign off to indicate that the data sent to the SAAS have been tested. The IRS has also initiated a process to track and more fully consider input from stakeholders as part of the audit plan process. Furthermore, the IRS has adjusted its guidance to better capture the relevant time zones for data being sent to the SAAS.

The ESAT office has made progress toward completing application audit plans, a necessary step to implement the enterprise audit trail solution. The ESAT office identified a total of 328 systems that should be sending audit trail data to the SAAS. Of these 328 systems, 158 were categorized as having completed audit plans in mid-May 2015, compared to 83 we previously reported in Fiscal Year 2012. Additionally, 32 unique systems were sending data to the SAAS in March 2015, compared to 14 unique systems in CY 2012.[8] In CY 2013 and CY 2014, the ESAT office helped system owners complete 30 audit plans, with 22 of them being completed in CY 2013 and eight being completed in CY 2014. Of the 30 completed audit plans, 23 were for higher priority systems, which included systems that processed taxpayer data. The ESAT office explained that fewer audit plans were completed in CY 2014 primarily because the number of its staff has declined over time. Also, a change in the mix of applications going through the audit plan process affected completions. At this pace, the ESAT office is on track to meet its goal with respect to completing audit plans for 50 percent of applications that process taxpayer data by CY 2021. However, while the audit plans are in the process of being completed, as we explain later, there are still some problems related to sending completed audit trails to the SAAS, which is part of the goal as well.

While these changes demonstrate that the ESAT office's commitment to improving its procedures, the IRS needs to take additional steps to more effectively address its audit trail issues. To improve the number and quality of audit trails sent to the SAAS, the IRS needs to

[8] The IRS counted a total of 49 systems or applications sending audit trail data to the SAAS in March 2015 and 20 systems or applications in CY 2012. Some of the audit trails were coming from the same system but were counted separately by the IRS, leading to a higher count compared to counting each unique system only once.

strengthen controls to ensure that: 1) information technology development projects coordinate with the ESAT office to ensure appropriate consideration of audit trail requirements; 2) once audit plans are completed, system owners stay engaged until sufficient audit trails are sent to the SAAS; and 3) any identified audit trail deficiencies are timely corrected.

Not All Systems in Development Adequately Considered Audit Plan Requirements

The Internal Revenue Manual[9] states that new systems or applications that require audit plans shall not be deployed without an approved audit plan fully implemented and tested through the enterprise life cycle process.[10] However, the majority of the new projects we reviewed did not meet this standard. Of the 61 projects that were coached by the Enterprise Life Cycle office and were in the process of exiting Milestone 4b from October 2011 to November 2014, the ESAT office determined that 29 should complete audit plans. Of those 29, only eight had signed audit plans at the completion of the enterprise life cycle process. Of those eight projects, only two also had an interface control document, which is needed to transmit to the SAAS, and had actually transmitted data to the SAAS even after several months of deployment. Consequently, many systems were put into production without fully functional audit trails.

To ensure that new systems or applications (or existing systems that are developing new releases) are deployed with compliant audit trails, the IRS has incorporated requirements for completing audit plans into its enterprise life cycle process. Milestone exit instructions indicate that a draft audit plan is required at Milestone 2 and a signed audit plan is required at Milestone 4a. These and other security-related artifacts[11] must be assessed at each milestone from one through five to ensure that information technology security needs have been appropriately addressed as projects progress through the milestones. The Enterprise Life Cycle office relies on the Cybersecurity Enterprise Federal Information Security Management Act[12]

[9] Internal Revenue Manual 10.8.3.4.2 (July 24, 2013).

[10] The enterprise life cycle is a framework used by IRS projects to ensure consistency and compliance with Government and industry best practices. This framework is the workflow that projects follow to move an information technology solution from concept to production while making sure that they are in compliance with IRS guidelines and are compatible with the overall goals of the IRS. The enterprise life cycle process is composed of multiple phases, each of which requires various milestone artifacts to be completed prior to exiting that milestone. The milestones are:

- Milestone 0: Vision and Strategy.
- Milestone 1: Project initiation.
- Milestone 2: Domain Architecture.
- Milestone 3: Preliminary Design (Logical Design).
- Milestone 4a: Detailed Design (Physical Design).
- Milestone 4b: System Development.

[11] An enterprise life cycle artifact is the tangible result (output) of an activity or task performed by a project during the life cycle.

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

(FISMA) Certification Program Office to review the security-related artifacts, called the Security Package, at each milestone and, if satisfied, to issue a memorandum to the Enterprise Life Cycle office recommending whether or not the project is cleared to exit the milestone.

New projects entering the enterprise life cycle are required to contact the ESAT office at Milestone 2 to assess the need for audit trails and audit plans.[13] The FISMA Certification Program Office, as well as guidance in the Internal Revenue Manual, informs the project offices that it is their responsibility to contact the ESAT office regarding audit trails and audit plans. The ESAT office told us that project offices must consult with them because sometimes project offices do not fully understand the guidance on what constitutes accesses to taxpayer information that should be sent to the SAAS.

However, the FISMA Certification Program Office indicated that new projects that are related to legacy systems are not always held to the same enterprise life cycle standards as brand new systems in regards to contacting the ESAT office or developing audit plans during the process. Generally, legacy systems that are already in production and waiting for the ESAT office's help to develop an audit plan are allowed time to get audit trails in place as scheduling, time, and resources allow. Therefore, the FISMA Certification Program Office may allow legacy systems to exit and deploy new releases without completing audit plans.

However, to ensure that system owners are fully aware of their audit trail requirements, we believe that all new projects entering the enterprise life cycle (including new releases of legacy systems) should contact the ESAT office as required early in the process. While some projects will not be required to have an audit plan, the ESAT office should make that determination. Currently, there is no formal control to ensure that project offices have contacted the ESAT office and actually obtained its input or had their projects assessed by the ESAT office. The ESAT Office indicated that project owners that do not meet with them may not provide enough information in their draft Audit Plans at Milestone 2 to ensure successful planning and implementation of audit trails by Milestone 4b. Although the ESAT office uses an initial meeting checklist with project owners that could validate that a discussion about audit trail requirements took place, the FISMA Certification Program Office does not get a copy of this checklist. Consequently, it does not have the information needed to determine if the draft audit plan has actually been discussed with the ESAT office prior to exiting Milestone 2.

Without the ESAT office's assessment of audit trail requirements early in the enterprise life cycle process, new projects may deploy without proper audit trails required for UNAX investigations or other purposes. Additionally, projects may be delayed in sending audit trails because the development phase did not include the full amount of planning needed for achieving compliant audit trails.

[13] Projects that consist of a new release of a prior project may start at a later phase, such as Milestone 3 or 4a, depending on individual project characteristics.

Recommendation

Recommendation 1: The Chief Technology Officer should ensure that the ESAT checklist is amended to include an ESAT office signature block to indicate that the project was evaluated for audit trail requirements prior to exiting Milestone 2 and that the checklist is then provided to the FISMA Certification Program Office as part of the Security Package. New projects related to legacy systems should not be exempt from this control.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS will amend the checklist to include a signature block and provide it to the FISMA Certification Program Office though not as part of the Security Package. The ESAT checklist is a required artifact for the enterprise life cycle milestone exit review. The review document has a signature block verifying that all required artifacts are properly completed. The IRS agreed that new projects related to legacy systems should not be exempt from this control, which is its current policy.

Even After Audit Plans Were Completed, Challenges Remained for Transmitting Audit Trails

In addition to the requirement for an audit plan, interface control documents are required for each application that must transmit audit trails to the SAAS. The SAAS collects, stores, and reports audit trail data for the investigation of potential instances of UNAX violations against IRS computer systems. The interface control document defines the mandatory SAAS fields and describes how fields will be populated by the application. The completion of the document is required in order to ensure that proper audit trail records are available for review and analysis by authorized users.

However, as mentioned previously, only two of the 29 projects that were in the process of exiting Milestone 4b (for which the ESAT office had determined audit plans were required) had an interface control document when exiting the enterprise life cycle process and had actually transmitted data to the SAAS, even after several months. We reviewed the status of the interface control documents for the eight projects that had signed audit plans and an additional 13 projects that had substantially completed audit plans. Our analysis showed that for 15 of the 21 projects, the document had not been started or was still in process. Consequently, many projects resulted in systems being put into production without fully functional audit trails. Some of these systems may have had separate application-level audit trails that were kept outside the SAAS, but these audit trails would not have met the IRS's requirements for UNAX-compliant audit trails.

The *Automated Solution Implementation Process* acknowledges the key role the interface control document plays in completing the audit trail process and that completing it is a time-consuming process requiring a level of effort of approximately 53 work days just on the part of the ESAT office/SAAS staff, which does not include the project owner's effort. The IRS told us that the obstacles to timely completion of the interface control document include: the project

development team's resource limitations, learning curve, and higher priorities; technical difficulties; the filing season moratorium on system changes; and communication issues between the various groups needed for successful completion of documentation and testing.

Despite its key role, the interface control document is not specified as an artifact that the FISMA Certification Program Office requires within the Security Package. Therefore, system owners may be delaying the completion of the interface control document as it is not specified as an artifact required for milestone exit prior to deployment.

With respect to sending data to the SAAS, it may not be practical to expect that project owners will always be able to complete the interface control document and transmit data to the SAAS prior to the system exit at Milestone 4b. However, the inability to timely send audit trails to the enterprise solution jeopardizes the IRS's goals for end-to-end auditing solutions. If audit trails are not sent to the SAAS or are inadequate, UNAX violations could occur and not be detected. Investigations may be impeded because audit trails are not fully operational in the SAAS. Ensuring that project owners follow through the entire process to send accurate and complete audit trails to the SAAS is critical to achieving enterprise audit trail goals.

Recommendation

Recommendation 2: The Chief Technology Officer should clarify guidance which specifies that preparing the interface control document is an integral task to sending audit trails to the SAAS. The guidance should include that the interface control document is the responsibility of the system owners and needs to be completed. In addition, the interface control document should be included as a Security Package artifact. If not completed prior to Milestone 4b exit, the interface control document and the SAAS testing/transmission tasks should be included in a system Plan of Action and Milestones[14] as an open deficiency that needs to be addressed.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has clarified guidance which specifies that the interface control document is an integral task to sending audit trails to the enterprise solution (SAAS). The guidance includes language which clarified that the interface control document is the responsibility of the system owner and should be completed before the audit plan is signed. The interface control document is included in the Security Package as an artifact. If not completed prior to Milestone 4b, the interface control document and the SAAS testing/transmission tasks should be included in a system Plan of Action and Milestones as an open deficiency that needs to be addressed.

[14] The Plan of Action and Milestones is a tool that identifies tasks that need to be accomplished; it details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. It is a key document used to track the status and the resolution of weaknesses or deficiencies noted in security controls during the security control assessment.

Improvements Are Needed to Ensure That Identified Audit Trail Deficiencies Are Timely Corrected

The Internal Revenue Manual[15] requires that all information technology security deficiencies warranting corrective actions that have been identified by internal or external evaluations of the IRS must be documented in a Plan of Action and Milestones within 60 calendar days.

In April 2013, the Director of Cybersecurity Architecture and Implementation issued a memorandum that shifted the responsibility for audit trail deficiencies on systems without fully implemented audit plans from system owners to the IRS at an enterprise level. The memorandum designated audit trail controls to be organizational common controls until an enterprise solution for audit trails was implemented. This effectively consolidated all IRS system and application audit trail deficiencies into one program-level Plan of Action and Milestones.[16] The intent of this program-level approach was to ease the burden on system owners for individual tracking of audit trail deficiencies until an enterprise solution was implemented. The memorandum stated that once a system had an ESAT-approved audit plan and the solution was fully implemented, the responsibility for meeting audit trail requirements would revert back to the system owner.

While working with system owners on completing audit plans, it is not unusual for the ESAT office to identify deficiencies that need to be corrected to ensure proper audit trails. These deficiencies include such matters as not capturing required events or data elements. The ESAT office began documenting the audit trail deficiencies it identified in system audit plans and instructing system owners to create a Plan of Action and Milestones for tracking progress to correct them. The ESAT office stated in the audit plans that the listed deficiencies were outside the scope of the program-level Plan of Action and Milestones and that it was the system owner's responsibility to create a system-specific Plan of Action and Milestones in the IRS's weakness repository and track progress to correct the deficiencies. The ESAT office also began to issue an audit notification memorandum to the system owners to highlight the need to correct the deficiencies or create a Plan of Action and Milestones within 60 calendar days. From May 2014 to January 2015, the ESAT office issued 10 audit notification memorandums.

Of the 10 system owners who received the audit notification memorandum, nine did not report deficiencies in the Plan of Action and Milestones within the 60 calendar days. Although not meeting time requirements, one of the nine system owners subsequently created a Plan of Action and Milestones for its system's audit trail deficiencies after more than 120 calendar days. In CY 2014, the ESAT office recorded audit deficiencies in three additional audit plans (but had not yet sent an audit notification memorandum). Of these three, two of the system owners did not create a Plan of Action and Milestones within the required 60 calendar days.

[15] Internal Revenue Manual 10.8.1.4.4.4 (Dec. 23, 2013).
[16] Program-level Plan of Action and Milestones weaknesses affect other applications, other business units, and organizations other than the organization responsible for implementing the control.

We spoke with the 10 system owners who received the audit notification memorandum, and they provided various reasons for why they did not create a Plan of Action and Milestones or move forward to correct the identified deficiencies. These reasons included:

- Confusion over how the Plan of Action and Milestones process works or the belief that it was the Cybersecurity office's responsibility to create the Plan of Action and Milestones (even at the system level).
- Disagreement that the deficiency belonged to the application but rather should be directed to a higher-level infrastructure or operating platform.
- The process to deal with the audit notification memorandum was new.
- The belief that action was not needed to correct the deficiencies listed in the audit plan until the ESAT office provided assistance in getting the audit trails transmitted to the SAAS.
- The audit notification memorandum "fell through the cracks."

The program-level Plan of Action and Milestones has contributed to the confusion on system owner responsibility. The memorandum does not clearly direct system owners to assume responsibility at the system level when the audit plan is completed. Rather, it states that the program-level Plan of Action and Milestones remains in effect until the audit plan is approved and "the enterprise solution is fully implemented." This has effectively delayed system owners who have an approved audit plan from taking responsibility to ensure that audit trails are actually transmitted to the SAAS and that any identified deficiencies are corrected.

In addition, because the program-level Plan of Action and Milestones allowed responsibility for audit trail controls to remain at the organization level, these controls were not being tested at the system level during the Cybersecurity office's annual testing of security controls even when an approved audit plan existed. Therefore, no audit trail deficiencies were reported even when they were listed in the audit plan.

Since the majority of the identified audit trail deficiencies were not placed into a Plan of Action and Milestones, the deficiencies were allowed to persist without visibility to higher-level IRS management who monitor the status of IRS security weaknesses, which could lead to these deficiencies persisting indefinitely. Consequently, with audit trail deficiencies remaining unresolved, IRS management may be unable to identify or substantiate noncompliant activity or hold employees accountable to UNAX policies.

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 3: The Associate Chief Information Officer, Cybersecurity, revises the program-level memorandum to clearly state that the responsibility for audit trail controls reverts to the system owner once the ESAT office has signed (approved) the audit plan.

> ***Management's Response:*** The IRS agreed with this recommendation. The Organizational Common Control memorandum has been revised stating that the responsibility for audit trail controls reverts to the system owner once the ESAT office has signed the audit plan.

Recommendation 4: System owners timely create a Plan of Action and Milestones for all identified information technology security weaknesses, including audit trail deficiencies.

> ***Management's Response:*** The IRS agreed with this recommendation. Using the processes contained in the IRS enterprise FISMA Plan of Action and Milestones Standard Operating Procedures, the Cybersecurity office will ensure that system owners timely create Plans of Action and Milestones for all information technology security weaknesses, including audit trail deficiencies.

Recommendation 5: The ESAT office issues an audit notification memorandum for deficiencies identified in previously completed audit plans if the system owner did not get one of the memorandums and there are no Plans of Action and Milestones for the deficiencies.

> ***Management's Response:*** The IRS agreed with this recommendation. The ESAT office has updated the process for identifying auditing deficiencies. Furthermore, for previously completed audit plans for which deficiencies were identified, no audit notification memorandums were issued, and there are no Plans of Action and Milestones for the deficiencies, the ESAT office has issued deficiency memorandums to application owners, authorizing officials, and Security Risk Management.

Recommendation 6: The Cybersecurity Security Risk Management office, which conducts annual testing of security controls, ensures that testers are instructed to appropriately test audit trail controls and report the identified audit trail deficiencies.

> ***Management's Response:*** The IRS agreed with this recommendation. The Cybersecurity office has updated its processes to ensure that audit trail deficiencies are identified via the Annual Security Controls Assessment's Security Assessment Report.

Unclear Procedures Caused Program-Level Plans of Action and Milestones to Be Misclassified

Office of Management and Budget (OMB) policy requires agencies to prepare Plans of Action and Milestones for all programs and systems for which an information technology security weakness has been found. Program officials must report their progress on remediation of Plans of Action and Milestones to the agency Chief Information Officer on a regular basis, at least quarterly. Effective remediation of these security weaknesses is essential to achieving a mature and sound information technology security program and securing information and systems.

Within the IRS, this quarterly reporting is accomplished through the Treasury FISMA Inventory Management System. The Treasury FISMA Inventory Management System is the official FISMA repository tool for all Department of the Treasury bureaus to house data as part of the Treasury Department's efforts to comply with the E-Government Act of 2002,[17] the National Institute of Standards and Technology, and OMB regulations and guidance. The IRS has entered both program- and system-level Plans of Action and Milestones into the Treasury FISMA Inventory Management System for tracking their remediation.

However, the IRS Cybersecurity office entered the program-level Plan of Action and Milestones for audit trails (and its other program-level Plan of Action and Milestones) into the Treasury FISMA Inventory Management System with an incorrect status of "disposal," which would cause the Treasury Department to not count them as active Plans of Action and Milestones. The Cybersecurity office believed that disposal was the proper status to prevent program-level Plans of Action and Milestones from being counted as actual systems in the Treasury FISMA Inventory Management System inventory.

We spoke with Treasury Department staff, and they said that the status should be left blank, not as "disposal," in order to ensure that the Plans of Action and Milestones are counted. The blank status would also prevent them from being counted as actual systems in the inventory. After being informed that the status should be blank, the IRS told us that it promptly corrected the statuses for all of its program-level Plans of Action and Milestones. The Cybersecurity office was not aware that the status should be left blank because the Treasury FISMA Inventory Management System user guide did not include instructions on this topic. Treasury Department staff said that the user guide will be updated to indicate that the status should be left blank in the case of program-level Plans of Action and Milestones.

If the Cybersecurity office had not corrected the status, the weaknesses identified in the program-level Plans of Action and Milestones could be overlooked by the IRS, the Department of the Treasury, and potentially the OMB (if it requested the information) and therefore remain uncorrected. We made no recommendation related to this finding because the IRS has already corrected the issue.

[17] Pub. L. No. 107-374.

Appendix I

Detailed Objectives, Scope, and Methodology

Our overall objectives were to evaluate the IRS's efforts to implement effective audit trails for new information systems that store and process taxpayer data and to track and correct identified deficiencies in existing audit trails. To accomplish our objectives, we:

I. Determined if the IRS has effective enterprise life cycle processes to ensure that audit plans are completed timely and accurately and that new systems deploy with effective audit trails.

A. Obtained IRS, OMB, and other guidance related to the enterprise life cycle.

B. Determined how audit trail requirements are integrated into the enterprise life cycle systems development process.

C. Assessed recently completed audit plans and related documents to determine if the ESAT office ensured that audit plans are accurate, complete, and compliant with requirements (as specified in Internal Revenue Manual 10.8.3) prior to signing. Specifically, reviewed procedures related to events, elements, collaborative efforts, and the audit plan template.

D. Evaluated the IRS's efforts to rectify the SAAS capacity issues.

E. For new systems that had entered Milestone 2 and exited Milestone 4b, validated that the audit plans were in place.

F. For systems with UNAX risk that recently completed the enterprise life cycle and are in production, determined if audit trails contain information that is sufficient for UNAX investigations.

G. Obtained current performance metrics for the ESAT office/SAAS (number of systems transmitting to the SAAS, number of systems with taxpayer data, number of audit trails verified to be sufficient, *etc.*).

H. Evaluated the ESAT office's current plan to achieve full end-to-end ESAT auditing by CY 2027 and determined what challenges exist in regard to the ESAT office achieving its goal.

II. Assessed if the ESAT office adequately addressed findings and recommendations from TIGTA's previous audit on UNAX audit trails.

   A. Reviewed the ESAT office's progress to improve processes to ensure event capture, complete elements (including timestamps), collaborative efforts, and documenting testing.

III. Determined if the IRS has adequately documented and monitored the audit trail weaknesses it has identified through the use of Plans of Action and Milestones or other means and is making progress in correcting those weaknesses.

   A. Obtained and reviewed the documented policies and procedures for managing Plans of Action and Milestones at all levels (enterprise/program/system/other), including guidance from the National Institute of Standards and Technology, the OMB, the Department of the Treasury, and the IRS.

   B. Interviewed IRS officials to determine how the IRS handles audit trails and the audit trail weaknesses it identifies. We evaluated when the system owners can reference organizational common controls or a program-level Plan of Action and Milestones.

   C. Interviewed the IRS to determine how the various levels of audit trail Plans of Action and Milestones are tracked in the Treasury FISMA Inventory Management System.

   D. Determined responsibility for and progress on audit trail and related controls and whether deficiencies were appropriately identified in findings memoranda and documented in Plans of Action and Milestones.

   E. Assessed if the program-level Plan of Action and Milestones and system audit trail weaknesses are included in appropriate reports.

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 objectives: Internal Revenue Manual Sections 2.16.1 and 10.8.3 and other IRS procedures for ensuring sufficient application audit trails are implemented. We evaluated these controls by interviewing management and reviewing relevant IRS documentation.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Mary Jankowski, Lead Auditor
Michael Mohrman, Senior Auditor
Midori Ohno, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Officer 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 Audit Coordination OS:PPAC:AC
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

Appendix IV

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

SEP 0 3 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report – Improvements Are Needed to Ensure New Information Systems Deploy With Compliant Audit Trails and Identified Deficiencies Are Timely Corrected, (Audit # 201520004) (e-trak #2015-71523)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased that your report acknowledged the IRS's continued progress in implementing an Enterprise audit solution, and closing the gap on weaknesses related to UNAX. Noteworthy efforts included the IRS taking a strategic management approach to prioritize application audit plans in a resource constrained environment. In addition, it was noted that procedural changes have been implemented to better highlight audit trail weaknesses to system owners during the audit log implementation process.

Despite resource constraints and fiscal challenges, the IRS is committed to continuously improving UNAX audit trails to detect and monitor unauthorized access and disclosure of taxpayer record. The attachment to this memo details our planned corrective actions to implement the audit report's recommendations.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (240) 613-9373 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment

Attachment

Draft Audit Report – Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and Identified Deficiencies Are Timely Corrected (Audit #201520004) (e-trak #2015-71523)

RECOMMENDATION #1: The Chief Technology Officer should ensure that the ESAT checklist is amended to include an ESAT office signature block to indicate that the project was evaluated for audit tail requirements prior to exiting ELC milestone 2, and then provided to the FISMA CPO office as part of the Security Package. New projects related to legacy systems should not be exempt from this control.

CORRECTIVE ACTION #1: The IRS partially agrees with this recommendation. We agree to amend the checklist to include a signature block and provide to the FISMA CPO office. The ESAT checklist is a required artifact for the ELC milestone exit review (MER). The MER exit document has a signature block verifying that all required artifacts are properly completed. The ESAT checklist is provided to the FISMA CPO. The IRS does not agree that the ESAT checklist is a part of the Security package. We agree new projects related to legacy systems should not be exempt from this control, and is the current policy.

IMPLEMENTATION DATE: June 15, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.

RECOMMENDATION #2: The Chief Technology Officer should clarify guidance which specifies that preparing the interface control document is an integral task to sending audit trails to the SAAS. The guidance should include that the interface control document is the responsibility of the system owners and needs to be completed. In addition, the interface control document should be included as a Security Package artifact. If not completed prior to Milestone 4b exit, the interface control document and the SAAS testing/transmission tasks should be included in a system Plan of Action and Milestones [1] as an open deficiency that needs to be addressed.

CORRECTIVE ACTION #2: IRS agrees with this recommendation. The IRS has clarified the guidance which specifies that the ICD is an integral task to sending audit trails to the enterprise solution (SAAS). The guidance includes language that clarifies the ICD is the responsibility of the system owner and should be completed before the audit plan is signed. The ICD is included in the Security Package as an artifact. If not completed prior to ELC milestone 4b exit, a system Plan of Action and Milestones (POA&M) will be opened.

IMPLEMENTATION DATE: June 15, 2015

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

---

Attachment

Draft Audit Report – Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and Identified Deficiencies Are Timely Corrected (Audit #201520004) (e-trak #2015-71523)

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.

RECOMMENDATION #3: The Chief Technology Officer should Ensure the ACIO Cybersecurity revises the program-level memorandum to clearly state that the responsibility for audit trail controls reverts to the system owner once the ESAT office has signed (approved) the audit plan.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The Organizational Common Control (OCC) memo has been revised stating the responsibility for audit trail controls reverts to the system owner once the ESAT office has signed the audit plan.

IMPLEMENTATION DATE: July 31, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.

RECOMMENDATION #4: The Chief Technology Officer should ensure system owners timely create POA&Ms for all identified IT security weaknesses, including audit trail deficiencies.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Using the processes contained in the IRS Enterprise FISMA POA&M SOP, Cybersecurity will ensure system owners timely create POA&Ms for all IT security weaknesses, including audit trail deficiencies.

IMPLEMENTATION DATE: December 15, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.

RECOMMENDATION #5: The Associate Chief Information Officer for Cybersecurity should ensure the ESAT office issues audit notification memorandums for deficiencies identified in previously completed audit plans if the system owner did not get one of the memorandums and there are no POA&Ms for the deficiencies.

Attachment

Draft Audit Report – Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and Identified Deficiencies Are Timely Corrected (Audit #201520004) (e-trak #2015-71523)

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. The ESAT PMO has updated the process for identifying auditing deficiencies. Furthermore, for previously completed audit plans where deficiencies were identified, in which no audit notification memorandums were issued and there are no POA&Ms for the deficiencies, ESAT has issued deficiency memorandums to application owners, Authorizing Officials (AOs) and Security Risk Management (SRM).

IMPLEMENTATION DATE: July 12, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.

RECOMMENDATION #6: The Chief Technology Officer should ensure that the Cybersecurity Security Risk Management office, which conducts annual testing of security controls, ensures that testers are instructed to appropriately test audit trail controls and report the identified audit trail deficiencies.

CORRECTIVE ACTION #6: The IRS agrees with the recommendation. Cybersecurity has updated its processes to ensure audit trail deficiencies are identified via the Annual Security Controls Assessment's Security Assessment Report.

IMPLEMENTATION DATE: May 22, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Accepted Corrective Actions are entered into the Joint Audit Management Enterprise System (JAMES) and monitored on a monthly basis, until completion.