TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

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

July 31, 2020

Reference Number: 2020-20-033

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

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

Final Audit Report issued on July 31, 2020
Reference Number 2020-20-033

Why TIGTA Did This Audit

This audit was initiated as a follow up to a Fiscal Year 2015 audit (TIGTA, Ref. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015)) that reported the IRS had not assessed audit trail requirements on some applications prior to deployment and had not ensured that some applications were transmitting audit trails to the audit trail repository in accordance with requirements when deployed.

Implementing audit trails has long been a challenge for the IRS. In Fiscal Year 1997, the IRS reported audit trails as an area of material weakness.

The overall objective of this audit was to determine whether the IRS has effectively implemented unauthorized access audit trail policies and procedures.

Impact on Taxpayers

Without effective audit and monitoring controls, the IRS's ability to establish individual accountability, monitor compliance with security and configuration management policies, and identify anomalous activity is reduced. In addition, without complete and accurate audit trails on all of its applications with sensitive data, unauthorized accesses, misuse, and theft of taxpayer data and Personally Identifiable Information could be occurring in IRS applications without detection.

What TIGTA Found

The IRS made some progress in implementing solutions to address audit trail weaknesses with the issuance of policies, procedures, and guidance and the completion of most of the corrective actions from TIGTA's prior audit on audit trail weaknesses. However, implemented audit trail solutions are not effective, and the IRS continues to have challenges with ensuring that all applications are providing complete and accurate audit trails for monitoring and identifying unauthorized access and for other investigative purposes.

Specifically, the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and Personally Identifiable Information. This inventory is critical as a baseline for all applications that need to be monitored for potential unauthorized access by employees. These applications are required to provide audit trail records to a repository used for investigative purposes. During the audit, TIGTA determined that 67 applications should be monitored for unauthorized access. Of these 67 applications, TIGTA determined that six (9 percent) applications were providing accurate and complete audit trails, 30 (45 percent) applications were providing incomplete and inaccurate audit trails, and 31 (46 percent) applications were not providing any audit trails to the repository.

In addition, not all applications with audit trail deficiencies were being tracked and monitored as required, which could allow unresolved deficiencies to persist indefinitely. Lastly, inconsistencies between internal policy and the Audit Trail Deficiency Memorandum may be a contributing factor to the untimely documentation of planned corrective actions for information technology security weaknesses identified by internal or external evaluations.

What TIGTA Recommended

The Chief Information Officer should ensure that a methodology is developed and implemented to identify and annually update the inventory of all applications that store or process taxpayer and Personally Identifiable Information for the purpose of detecting improper cyber activities and to reconstruct events for potential criminal investigations, ensure that audit trail deficiencies are properly tracked and monitored as required, and ensure the internal policy and the Audit Trail Deficiency Memorandum template document clearly and consistently communicate each stakeholder's responsibilities to ensure that the appropriate actions are taken when security weaknesses have been identified.

The IRS agreed with four of our recommendations and plans to properly track audit trail deficiencies, clearly and consistently communicate stakeholder's responsibilities, and document process improvements. However, in the partially agreed-to recommendation, the IRS does not plan to clearly identify applications that use Personally Identifiable Information for the purpose of detecting improper activities and to reconstruct events for potential criminal investigations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 31, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information (Audit # 201920006)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has effectively implemented unauthorized access audit trail[1] policies and procedures. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

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

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 R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

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

Table of Contents

Background

An audit trail[1] or audit log generally refers to a record of events[2] occurring on a computer system. Audit trails can maintain a record of system activity both by system and application processes and by user activity of the same. Being able to reconstruct and determine what events occurred on a system is crucial to establishing individual accountability, monitoring compliance with security policies, identifying malicious activity, and investigating security violations.

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.

Federal Government, Department of the Treasury, and Internal Revenue Service (IRS) 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. Policies also require the periodic review of information system audit trail transactions. In addition, because of the sensitivity of tax return information, Internal Revenue Code Section (§) 6103[3] and the Taxpayer Browsing Protection Act of 1997[4] place an additional responsibility on the IRS to protect taxpayer information from unauthorized inspection and disclosure. The willful unauthorized access or inspection of taxpayer records is a crime punishable upon conviction by fines, prison terms, and termination of employment. IRS security policies require that, at a minimum, audit trails must include sufficient information to establish what events occurred, when the events occurred, and who (or what) caused them.

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. In March 2010, the IRS established the Enterprise Security Audit Trails (ESAT) Project Management Office (hereafter referred to as the ESAT office) within the Information Technology organization's Cybersecurity function. The ESAT office's mission is to protect Sensitive But Unclassified data, including taxpayer information and IRS electronic systems, services, and data, from internal and external cybersecurity-related threats by implementing security practices in planning, implementation, risk management, and operations. The ESAT office established the following processes:

- The Security Audit and Analysis System (SAAS) was created to act as a centralized data repository to collect audit logs from various applications. All IRS applications containing taxpayer data and Personally Identifiable Information (PII), which consists of taxpayer, financial, or employee information that identifies a taxpayer or entity, are required to send their application transactions (audit trails) to the SAAS.

[1] See Appendix IV for a glossary of terms.
[2] An event is any action that happens on a computer system. Examples include logging into a system, executing a program, and opening a file.
[3] Internal Revenue Code § 6103 is the section of the code that restricts the disclosure of tax returns and return information.
[4] Pub. L. 105-35, 26 USC §§ 7213, 7213A, 7431.

- The SAAS collects key information necessary to detect improper cyber activities and to reconstruct events for potential criminal investigations. This information is processed so that authorized users can generate reports and create custom queries for their various purposes. Authorized users include the Treasury Inspector General for Tax Administration (TIGTA), IRS Criminal Investigation, and Cybersecurity function Security Operations function personnel.

  For example, one of the SAAS users is a group in the TIGTA Office of Investigations (OI) comprised of an analyst and computer specialists. This group is primarily responsible for identifying and developing new automated scenarios to detect unauthorized accesses of tax information in the newly modernized IRS computer systems. In addition, TIGTA OI reviews applications that contain PII and no tax information because the applications are also subject to unauthorized access, theft, and misuse.

In a Fiscal Year 2015 audit report, TIGTA reported[5] that the IRS continued to make progress in implementing its enterprise solution to address its audit trail deficiencies. However, the IRS needed 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 the IRS had not assessed audit trail requirements on some IRS systems prior to deployment. Of the systems with a completed audit plan during the development process, most were not transmitting audit trails in accordance with requirements when deployed. TIGTA made six recommendations to address these findings.

Results of Review

The IRS made some progress in implementing solutions to address audit trail processing and the prior recommendations, which is presented in detail further in the report. However, we believe implemented audit trail solutions are not effective and significant improvements are still needed in the following areas:

- There is not an accurate inventory of and effective audit trails for all applications that store or process taxpayer data and PII.
- Audit trail weaknesses identified in Audit Trail (AU)[6] Deficiency Memorandums (hereafter referred to as the *AU Deficiency Memo*) were not always tracked in a plan of action and milestones (POA&M).

Without effective audit and monitoring controls, the IRS's ability to establish individual accountability, monitor compliance with security and configuration management policies, and identify anomalous activity is reduced. In addition, without fully operational audit trails or no audit trails, unauthorized accesses, misuse, and theft of taxpayer data and PII could be occurring in IRS applications without detection.

[5] TIGTA, Ref. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015).
[6] The National Institute of Standards and Technology defines the Audit Trail category with the letters "AU."

There Is Not an Accurate Inventory of and Effective Audit Trails for All Applications That Store or Process Taxpayer Data and Personally Identifiable Information

The IRS could not provide an accurate inventory of all applications that store or process taxpayer data and PII available for monitoring and the investigation of unauthorized accesses by employees

During the audit, we encountered many challenges in trying to determine the number of IRS applications storing or processing sensitive information that should be monitored for unauthorized access by employees and contractors. We obtained different inventory lists from various offices at different points of the audit. For example, in March 2019, we received an inventory list of 155 applications from the ESAT office, and a month later, we received an inventory list of 167 applications from business units across the IRS. In November 2019, we received the inventory list that contained 48 applications from the Privacy, Governmental Liaison, and Disclosure office. Throughout the audit, TIGTA OI also provided us with the inventory of applications with which it was working.

Maintaining a current and accurate inventory of applications is essential to ensure that systems with sensitive information are being monitored for unauthorized access.

We collaborated and worked with TIGTA OI and the IRS and determined there are 67 applications that store or process taxpayer data and PII that should be capturing and sending audit trails to the SAAS for unauthorized access monitoring and investigations. Four (6 percent) of the 67 applications that stored or processed taxpayer data were not on TIGTA OI's inventory list. According to the Privacy Impact Assessment performed on the four applications, they are Federal Information Security Modernization Act of 2014 (FISMA)[7] reportable systems. In addition, the 67 applications included 28 (42 percent) applications that were on TIGTA OI's inventory but not on the IRS's inventory lists.

The importance of maintaining a current and accurate inventory of applications is essential to ensure that applications with sensitive information are being monitored for unauthorized access. The *Standards for Internal Controls in the Federal Government*[8] requires that management design control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. The objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction. Availability means that data, reports, and other relevant information are readily available to users when needed.

[7] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.
[8] Government Accountability Office, GAO-14-704G, *By the Comptroller General of the United States: Standards for Internal Control in the Federal Government* p. 60 (Sept. 2014).

Audit trails for applications that store or process taxpayer data and PII have insufficient content and are not always timely reviewed and updated

As stated earlier, the SAAS is the system owned by the Information Technology organization and used by various stakeholders, such as TIGTA OI, IRS Criminal Investigation, and Cybersecurity function Security Operations function personnel, for different investigative purposes. Because of this, it is imperative that the SAAS is as complete, up-to-date, and accurate as possible.

However, the SAAS did not contain information for all applications and did not have sufficient audit trail information. Of the 67 applications that store or process taxpayer data or PII, we found the following:

- 6 (9 percent) applications had accurate and complete audit trails in the SAAS.
- 30 (45 percent) applications were sending deficient audit trails to the SAAS. The missing data included the success or failures of events, Internet Protocol address of the user initiating an event, Master File tax codes, Taxpayer Identification Numbers, and tax periods.
- 31 (46 percent) applications were not sending audit trail information to the SAAS.

Without complete and accurate audit trails from all systems that store or process taxpayer data and PII, TIGTA OI and IRS efforts to monitor the applications for unauthorized accesses or conduct investigative activities may be limited.

We requested the Audit Control Responses (ACR) for the 30 deficient applications to determine whether the application owners and the ESAT office are reporting and capturing the deficiencies as required. We found the ACRs for 21 (70 percent) applications that listed the missing data and nine (30 percent) applications that did not.

The ESAT office Audit Control Responses Standard Operating Procedures (hereafter referred to as procedures) states that every interaction with PII (taxpayer, employee, financial) that identified an individual or an entity through an application is an event and shall be audited. It further states that all IRS applications shall capture and record the minimal events, which include successes and failures of application critical record changes. We are not making any recommendations for the 30 applications that were sending deficient audit trails or the 31 applications that were not sending any audit trails to the SAAS because all 61 are audit trail deficiencies that can be addressed by the POA&M process presented later in this report.

We also reviewed the Organizational Common Controls Security Plans dated June 26, 2017, and June 21, 2019, to determine whether the IRS reviewed and updated the list of auditable events at the organization level, at a minimum of every two years as required.[9] We determined that the reviews were conducted timely. However, ESAT office procedures require application owners to perform an additional analysis to determine the criteria for which the audit events specific to their applications are implemented. That criteria should be based on the latest Internal Revenue Manual (IRM) guidance, which was May 5, 2019. The application owners are to capture the outcome of their detailed analysis in the ACR template. Once the ACR is developed, the application owner is responsible for ensuring that it is revalidated annually. If there are no

[9] Internal Revenue Manual 10.8.1.4.3.1.1., *AU-2 Audit Events – Control Enhancements* (May 9, 2019).

changes to the security auditing posture of the application, the revalidation checklist provided by the ESAT office should be returned to the audit trails mailbox.

We reviewed 30 applications and determined that for 17 (57 percent) applications, the audit events were aligned with the updated IRM 10.8.1. However, the audit events for the remaining 13 (43 percent) applications referenced the obsolete IRM 10.8.3. The range of the dates on the ACRs were from April 28, 2011, to December 14, 2016. We did not obtain the revalidation checklist to determine whether the ESAT office provided the application ACR revalidation checklist as required. However, the IRS acknowledged that the requirement to notify the ESAT office that the ACR does not require updating had not been enforced.

The causes of the conditions we identified can be attributed to management turnover, *i.e.*, the change in ESAT office management teams, which resulted in the loss of program continuity, loss of contractors, staff shortages, and the IRS's efforts to transition from the SAAS to the Splunk repository tool. In March 2019, we determined that the ESAT office had seven staff working audit trails. Two of the seven staff have more than two years of experience, while the remaining five staff have less than two years of experience. ESAT office employees stated they relied on TIGTA OI's inventory list, including its analysis of the applications that send or do not send information to the SAAS, because they do not have the staff to make that determination themselves. There is only one ESAT office employee who reviews and updates the inventory list, if time permits.

In Calendar Year 2018, personnel from both the ESAT office and TIGTA OI met and came up with some ideas to improve the workflow processes between both parties; however, due to limited resources resulting in the loss of contractors and a staff shortage, the momentum from their efforts did not continue and improvements did not come to fruition.

The IRS needs to significantly improve the security management of its applications that store or process taxpayer data and PII regarding making audit trails available for monitoring and investigative purposes. Because complete and accurate audit trails are not available for all applications, the IRS cannot ensure that it or TIGTA OI can sufficiently investigate security violations or unauthorized accesses by employees and contractors on all applications where taxpayer data or PII reside. In addition, having audit trails on all applications with taxpayer data and PII allow the IRS to meet its responsibility to protect taxpayer information from unauthorized inspection and disclosure as required by the Internal Revenue Code § 6103 and the Taxpayer Browsing Protection Act of 1997. From Fiscal Years 2017 to 2019, TIGTA OI investigated 394 cases of unauthorized accesses. This capability will be significantly enhanced when audit trails on all applications are available on the SAAS.

The Chief Information Officer should:

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

> **Management's Response:** The IRS partially agreed with this recommendation. The Cybersecurity function will partner with Privacy, Government Liaison, and Disclosure office to review and revise the current Privacy Impact Management System to clearly

identify applications that store, process, or transact Federal tax information for the purpose of detecting improper cyber activities and to reconstruct events for potential criminal investigations. This inventory will be updated, at a minimum, annually. The IRS will be replacing the SAAS; however, audit trails records will continue to be tracked in a centralized system.

> **Office of Audit Comment:** The IRS plans to identify and annually update the inventory of all applications that store, process, or transact taxpayer data. However, applications that store, process, or transact PII are not included in the planned corrective action. We believe the inclusion of applications that use PII in the inventory is important because unauthorized accesses to PII could result in identity theft and other financial improprieties, and the IRS's internal guidelines state that every interaction with PII (taxpayer, employee, financial) that identified an individual or an entity through an application shall be audited. In addition, IRS replacement of the SAAS is currently scheduled for completion in Calendar Year 2026. In the interim, the IRS needs to track the audit trail records in the SAAS, as recommended, or in a centralized location.

Recommendation 2: Obtain the list of 13 applications with an ACR that references the obsolete IRM, conduct a revalidation of the auditable events, and issue an AU Deficiency Memorandum to the application owner, if needed, to require an ACR update to comply with the current list of auditable events. In addition, ensure that revalidations are conducted annually as required.

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

Audit Trail Weaknesses Identified in Audit Trail Deficiency Memorandums Are Not Always Tracked in a Plan of Action and Milestones

Identified audit trail deficiencies are not always tracked in a POA&M. Using the 30 applications with deficient audit trails and 28 applications with no audit trails being sent to the SAAS,[10] we determined that the IRS is not creating the POA&Ms for all audit trail deficiencies and uploading the POA&Ms into the Treasury FISMA Inventory Management System as required. The AU Deficiency Memorandum provides the results of the ESAT office's review of the documentation for the audit security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. In

IRS policies and procedures require all information technology security weaknesses warranting corrective actions must be documented in a POA&M within 60 calendar days.

[10] There were three applications on the December 2019 updated TIGTA OI inventory that were not on the January 31, 2019, inventory list that we used to obtain the AU Deficiency Memorandums to conduct our analyses.

addition, IRS policies and procedures require all information technology security weaknesses warranting corrective actions that have been identified by internal or external evaluations must be documented in a POA&M within 60 calendar days.

We obtained 32 AU Deficiency Memorandums from the 30 applications[11] with deficient audit trails and 26 AU Deficiency Memorandums from the 28 applications with no audit trails. The AU Deficiency Memorandums were issued in Calendar Years 2015 through 2018.

For the 32 AU Deficiency Memorandums, we found:

- 20 (63 percent) AU Deficiency Memorandums were tracked in a POA&M. Seven (35 percent) POA&Ms were timely prepared within the 60-calendar-day requirement; however, 13 (65 percent) were untimely prepared with a range of 24 to 1,099 calendar days. This condition was included in the Fiscal Year 2015 TIGTA report along with a recommendation for the IRS to take action.
- 11 (34 percent) AU Deficiency Memorandums were not tracked in a POA&M.
- 1 (3 percent) AU Deficiency Memorandum was not required to be tracked in a POA&M.

For the 26 AU Deficiency Memorandums, we found:

- 20 (77 percent) AU Deficiency Memorandums were tracked in a POA&M. Three (15 percent) were timely prepared and 17 (85 percent) were untimely with a range of 29 to 1,319 calendar days.
- 6 (23 percent) AU Deficiency Memorandums were not tracked in a POA&M.

The ESAT office has been sending copies of the AU Deficiency Memorandums to the Enterprise FISMA Services (EFS) function since June 30, 2018. The EFS function started working the AU Deficiency Memorandums in February 2019; however, this work is time-consuming because there is only one dedicated resource to perform this task. As of November 2019, the EFS function received 14 AU Deficiency Memorandums from the ESAT office (11 in Calendar Year 2018 and three in Calendar Year 2019). We reviewed the 11 AU Deficiency Memorandums issued in Calendar Year 2018 and found that five applications had the POA&Ms, four applications had no POA&Ms, and two applications were not required to submit a POA&M. We also determined that the POA&Ms continued to be prepared in an untimely manner. To determine why the POA&Ms were not created for the four applications and why some POA&Ms were not prepared timely, we interviewed the applications' authorizing officials or authorizing official designated representatives. They offered various explanations on why POA&Ms were not created or not prepared timely.

- No POA&M was required because the deficiency was resolved two calendar days after the AU Deficiency Memorandum was issued. However, the EFS function and TIGTA OI had not updated their records.
- A POA&M was in the Treasury FISMA Inventory Management System but was 157 calendar days late because the decision was made to not address the deficiency until the application's next FISMA cycle, *i.e.*, when the security controls assessment was due.

[11] An application can have more than one AU Deficiency Memorandum.

- The ESAT office did not send the AU Deficiency Memorandum to the point of contact responsible for taking the appropriate action.
- The e-mail communication that included the AU Deficiency Memorandum was unclear to instruct the information technology specialist to take an action other than forward the AU Deficiency Memorandum to the authorizing official.
- Project personnel were not familiar with the ESAT office, and ESAT office procedures link in the AU Deficiency Memorandum did not work. In addition, there was no further engagement with the ESAT office after the audit plan or the ACR was developed.
- The audit control deficiency was not addressed due to other business priorities.
- The unified work requests to fix the code for the audit deficiencies were constantly denied by the Information Technology organization because of a lack of resources or funds and other higher priorities than correcting legacy applications. In addition, no POA&M was created because the end date could not be determined due to the unified work request denials.

Inconsistencies between internal policy and the AU Deficiency Memorandum may be a contributing factor to the untimely POA&Ms

We believe the inconsistent narrative in the IRM 10.8.1.4.4.4(2)[12] and the AU Deficiency Memorandum may be contributing to the untimely preparation of the POA&Ms. The IRS stated it determines when the POA&Ms should be developed based on IRM 10.8.1.4.4.4(1) and (2), which states:

> *Develop a POA&M for IRS information systems to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. All POA&Ms shall be entered into the Treasury FISMA reporting tool within 60 calendar days.*

The IRS considers the assessment of the security controls occurs when the security control assessment is conducted, which is based on the FISMA cycle. However, we determined that the POA&Ms should be developed based on the same IRM section but in (4)d and (6), which states:

> *The IRS shall document in POA&Ms, at a minimum, all IT cybersecurity weaknesses warranting corrective actions that have been identified by Internal IRS evaluations (e.g., policy, training programs, self-assessments, periodic security test and evaluation, or contingency plan testing). The IRS shall ensure that all new weaknesses are entered into appropriate POA&Ms within 60 calendar days of identification.*

We reviewed several additional Federal guidelines such as Treasury Directive 85-01, dated September 12, 2019, that states, "Bureau CISOs shall establish and maintain a process to track, for all cybersecurity weaknesses reported under self-assessments, external reviews, continuous monitoring activities, and other internal or external assessments." The Office of Management and Budget Memorandum-04-14, dated November 18, 2013, has similar language as the Treasury Directive. The IRS Request for Risk Acceptance and Risk Based Decision Standard Operating Procedures dated April 5, 2019, states, "For a security weakness identified outside an established Cybersecurity risk assessment process, the authorized official must decide to either

[12] IRM 10.8.1.4.4.4(2) *CA-5 Plan of Action and Milestones* (May 9, 2019).

fix the finding or accept the risk within 60 calendar days of identification. If the project determines mitigation is available or required, a POAM item must be created within the Treasury FISMA Information Management System **and** an assessment of risk performed." We concluded and believe that the most expedient process is for all information technology security weaknesses warranting corrective actions that have been identified by internal or external evaluations to be documented in a POA&M within 60 calendar days.

We also reviewed the AU Deficiency Memorandum template document, which clearly states that the application owner or authorizing official must address the deficiencies and that, according to IRM 10.8.1.4.4.4(2), they must create a POA&M in the Treasury FISMA Inventory Management System within 60 calendar days. However, further down in the same document, the following narrative is added:

> *Application audit control deficiencies are also provided to the Cybersecurity, Security Risk Management, Enterprise FISMA Compliance Office for assessment in the next applicable FISMA cycle.*

We believe the policy narrative and the above text could prompt the owner/authorizing official to delay preparing a POA&M until the previously referenced assessment is conducted.

Based on our discussions with the authorizing official designated representatives and security personnel, we believe that the timeliness of handling audit control deficiencies should improve if the previously mentioned perspectives and the apparent policy conflict are appropriately addressed, along with allowing some time for the current process to become institutionalized within the vested IRS organizations.

When audit trail deficiencies are not timely placed in a POA&M as required, IRS higher level management cannot effectively monitor the status of IRS security weaknesses. In addition, these deficiencies could go unresolved and persist indefinitely. Consequently, when audit trail deficiencies remain unresolved, IRS management may be unable to identify or substantiate noncompliant activity or hold employees accountable to unauthorized access policies.

The Chief Information Officer should:

Recommendation 3: Ensure that application audit trail deficiencies are properly tracked on a POA&M, thus ensuring compliance with the FISMA, IRM policy, and the Office of Management and Budget annual guidance.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function will ensure that currently identified application audit trail deficiencies are properly tracked in a POA&M in accordance with the FISMA, IRM policy, and the Office of Management and Budget annual guidance.

Recommendation 4: Ensure that the IRM policy and the AU Deficiency Memorandum template document clearly and consistently communicate each stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the POA&M is reflective of the issues indicated in the AU Deficiency Memorandum within 60 calendar days.

> **Management's Response:** The IRS agreed with this recommendation. The policy is in place and compliant with National Institute of Standards and Technology and Department of the Treasury audit trail controls. The AU Deficiency Memorandum

template will be revised to clearly and consistently communicate stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the POA&M is reflective of the issues indicated in the AU Deficiency Memorandum within 60 calendar days.

Recommendation 5: Establish a process improvement so application owners timely create the POA&Ms when audit trail deficiencies are identified. This recommendation also addresses a similar repeat finding from the Fiscal Year 2015 audit report previously mentioned.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity function will document within the POA&M Standard Operating Procedures process improvements to require that application owners create the POA&Ms timely when audit trail deficiencies are identified.

Office of Audit Comment: The IRS's response did not elaborate on the process improvements to ensure that application owners timely create the POA&Ms when audit trail deficiencies are identified. We believe the process improvements should include monitoring, analysis, and a methodology to measure the timeliness of creating the POA&Ms.

Some Progress Was Made to Address Audit Trail Processing

The IRS made some progress in implementing solutions to address audit trail processing with the issuance of policies, procedures, and guidance and the completion of most of the corrective actions to address weaknesses included in the Fiscal Year 2015 TIGTA report.

Policies, procedures, and guidance issued to address audit trail processing

In August 2017, TIGTA OI expressed concerns to the IRS on the IRS's decision to retire the IRM policy that required applications to log and capture any interaction with taxpayer data. TIGTA OI believed that without the policy, applications currently in development would not put adequate audit trails into production. In December 2017, the Cybersecurity function issued interim guidance updating its security policies to ensure that all necessary National Institute of Standards and Technology and Department of the Treasury requirements from the old policy would be carried over into its new policy. It specifically included the requirement that all projects and programs with audit plans in any state of development must take steps to migrate audit plan content into their system security plans. When this interim guidance expired in December 2018, the IRS was closed because of the 35-day Federal Government shutdown. In May 2019, the IRS Chief Information Officer issued IRM 10.8.1[13] that covered audit trail requirements on all systems and applications. Although approximately five months elapsed between the end of the interim guidance and the issued guidance, we did not identify any known effect directly related to this lapse.

On June 30, 2018, as a supplement to the overall IRM audit trail requirements, the ESAT office revised the AU Deficiency Memorandum to clarify the application owner's responsibility to correct audit deficiencies and made changes to the Cybersecurity EFS function's responsibilities. The ESAT office implemented a new process as follows:

[13] IRM 10.8.1.4.3.1.1., *AU-2 Audit Events – Control Enhancements* (May 9, 2019).

- When an application has an audit trail deficiency, the ESAT office will send the AU Deficiency Memorandum to the EFS function. The AU Deficiency Memorandum provides the ESAT office's results from its review of documentation of the audit security controls. The review determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements.
- The EFS function is responsible for managing the POA&Ms enterprise-wide. The EFS function e-mails the application's point of contact that he or she has 60 calendar days to develop a POA&M if the audit deficiency cannot be corrected within the specific time frame based on the Federal Information Processing Standards 199 category. In addition, the EFS function tracks the AU Deficiency Memorandum to ensure compliance with POA&M requirements.

Figure 1 shows the improvement that the IRS made in Calendar Year 2018 (shaded) as compared to the previous three calendar years with timely creating the POA&Ms in the Treasury FISMA Inventory Management System to address the applications with deficient audit trails.

Figure 1: Timeliness of POA&M Preparation Based on AU Deficiency Memorandum Issuance for Calendar Years 2015 Through 2018

Calendar Year	AU Deficiency Memorandum Issued (POA&M expected unless otherwise noted)	POA&M Not Prepared	POA&M Prepared	
			Untimely	Timely
2015	10	3	6	1
2016	7	3	4	0
2017	4[14]	1	2	0
2018	11	4	1	6
Total	**32**	**11**	**13**	**7**

Source: TIGTA's review of IRS AU Deficiency Memorandums from Calendar Year 2015 through 2018, the corresponding POA&Ms, and security documentation.

Other examples of progress include the ESAT office's June 3, 2019, issuance of ESAT office procedures to ensure that its guidance is consistent with National Institute of Standards and Technology guidance. The procedures cover guidance applicable to the collection and processing of computer-generated audit trails or audit logs. It includes the roles and responsibilities specific to the implementation of IRS Information Technology organization audit logging security. For example:

- The business and functional unit owners ensure that audit logs are collected and maintained for each IRS system. They ensure that a risk assessment is completed and information security audit requirements are documented in an approved ACR.
- The Associate Chief Information Officer, Cybersecurity, maintains and provides updates to the procedures. The Cybersecurity function is to provide guidance in the development of the ACRs for all IRS applications, in accordance with the procedures.

[14] A POA&M was not required for one AU Deficiency Memorandum issued in Calendar Year 2017.

The ESAT office owns the audit policy, communicates and interprets audit control requirements, and provides audit deficiencies as identified with applications.

- System, network, and database administrators enable and configure audit logging and infrastructure audit and control responses on all IRS systems in accordance with IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.[15]

***Management Action*:** After the completion of our fieldwork, a Cybersecurity function official provided TIGTA with a strategy plan, known as Next Gen ESAT, dated September 18, 2019. While we did not evaluate the Next Gen ESAT plan, we noted that the Next Gen ESAT will be an enterprise cybersecurity consolidated audit management system that will centralize enterprise audit, transaction, and infrastructure log events. It will enable the IRS to analyze information for system monitoring, cybersecurity management, and situational awareness, which the IRS states will be used for making informed business decisions. The scope of the Next Gen ESAT will include the enterprise collection of audit log data from operating systems, network components, *i.e.*, switches, routers, firewalls, *etc.*, and application transaction logs. Once the data collection is centralized within the Splunk® monitoring tool, all existing tools used to collect the audit log data can be decommissioned. Next Gen ESAT, which is being implemented in three phases, is currently in the first phase, the Limited Initial Operating Capability phase. The entire solution is estimated to conclude in Fiscal Year 2026.

Implemented planned corrective actions generally addressed the reported weaknesses for the prior TIGTA recommendations

Of the six recommendations from the Fiscal Year 2015 TIGTA audit report, the IRS fully implemented the planned corrective actions for five recommendations. The remaining recommendation was addressed earlier in this report. The fully implemented recommendations were:

- *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.*

  We confirmed that the IRS amended the ESAT audit trail checklist to include the signature block. While our review of one eligible application that exited Milestone 2 did not include a signature, the IRS provided an e-mail as evidence of the ESAT office's involvement. Although the IRS did not always use the signature block, we concluded that the project was evaluated for audit trail requirements.

- *The Chief Technology Officer should clarify guidance, which specifies that preparing the Interface Control Document (ICD) is an integral task to sending audit trails to the SAAS. The guidance should include that the ICD is the responsibility of the system owners and needs to be completed. In addition, the ICD should be included as a Security Package artifact. If not completed prior to Milestone 4b exit, the ICD and the SAAS testing/transmission tasks should be included in a system POA&Ms as an open deficiency that needs to be addressed.*

[15] IRM 10.8.2 (Sept. 30, 2016).

We agreed that the guidance clarified that the ICD is an integral task and that the ESAT office's procedures show that the information system security officer and the authorizing official are the owners. We concluded that ownership yields responsibility. SAAS ICD requirements provide that, if the application processes PII, an ESAT office SAAS-specific ICD may be required. It further specifies that the ICD will also need to be tested and the application should be activated in the SAAS for event collection. The IRS also provided the POA&Ms that addressed the deficient audit trail requirements for the applications tested. Therefore, we concluded that the recommendation was fully implemented.

- *The Chief Technology Officer should ensure that the Associate Chief Information Officer, Cybersecurity, revise the program-level memorandum to clearly state that responsibility for audit trail controls revert to the system owner once the ESAT office has approved the audit plan.*

  We reviewed the FISMA Security Controls Assessment Standard Operating Procedures, dated April 3, 2018, and verified that the recommendation was fully implemented.

- *The Chief Technology Officer should ensure that 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 memoranda and there are no POA&Ms for the deficiencies.*

  We identified one application in the Fiscal Year 2015 TIGTA report that did not have an audit notification memorandum. We reviewed the application's September 26, 2018, audit plan and no deficiencies were noted. Therefore, we concluded that the deficiencies had been addressed, and the recommendation is fully implemented.

- *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.*

  We reviewed ESAT office procedures and the procedures require that application ACR deficiencies are provided to the Cybersecurity, Security Risk Management, Enterprise FISMA Compliance office. The deficiencies will be scheduled for assessment by the Cybersecurity function team in the next FISMA cycle at which time either the deficiency will be discarded or a security assessment report will be provided. If an assessment report is provided, the deficiency is updated to a finding and a POA&M may be required. To confirm implementation of the procedures, we verified that the IRS selected and reviewed controls, including audit controls, as part of our annual FISMA review in Fiscal Years 2018 and 2019.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has effectively implemented unauthorized access audit trail policies and procedures. To accomplish our objective, we:

- Determined whether written policies and procedures for audit trails were compliant with Federal guidelines including National Institute of Standards and Technology guidance by reviewing IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*,[1] ESAT office procedures; and SAAS Concept of Operations.
- Determined whether the IRS timely updated IRM 10.8.1 to include audit and accountability requirements as they related to audit trails, and determined whether the IRS submitted reports on its progress regarding implementing audit trail requirements.
- Determined whether the IRS developed and implemented sufficient audit trail capabilities on all its applications that store or process taxpayer data by obtaining information from the IRS on all applications that store or process taxpayer data or PII that require audit trails, and compared this information with an inventory list obtained from TIGTA OI of IRS applications that require audit trails for monitoring unauthorized access.
- Determined which applications have complete audit trails, partial audit trails, or no audit trails. For applications with no or partial audit trails, we assessed whether these deficiencies have been identified in AU Deficiency Memorandums and identified possible causes.
- Determined whether the IRS has adequately tracked audit trail deficiencies through the POA&M process for resolution. We traced audit trail deficiencies from the ESAT office's AU Deficiency Memorandums to the corresponding POA&Ms. If no POA&M exists, we determined why by reviewing system security documentation and discussed the deficiency with Cybersecurity function personnel and the application business owner.
- Determined whether the IRS effectively implemented corrective actions for recommendations in a prior report to address audit trail issues by obtaining information from the Joint Audit Management Enterprise System for all closed recommendations and assessing whether the corrective actions were implemented and effectively addressed the reported weakness.

Performance of This Review

This review was performed with information obtained from the IRS Information Technology organization ESAT office and the Cybersecurity functions located in Austin, Texas, and in Lanham, Maryland, respectively, and from the TIGTA OI group located in Cincinnati, Ohio, during the period December 2018 through December 2019. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require

[1] IRM 10.8.1 (May 9, 2019)

that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Kent Sagara, Director; Deborah Smallwood, Audit Manager; Charles Ekunwe, Lead Auditor; Esther Wilson, Senior Auditor; and Linda Nethery, Information Technology Specialist.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: ESAT office procedures; IRM 10.8.1, *Information Technology Security, Policy and Guidance*; Treasury Directives 25-08 and 85-01; the Office of Management and Budget Memorandum-14-04; the IRS Request for Risk Acceptance and Risk Based Decision Standard Operating Procedures; SAAS Concept of Operations; and National Institute of Standards and Technology Special Publication 800-12, Revision 1, *An Introduction to Information Security*. We evaluated these controls by interviewing Cybersecurity function and ESAT office staff; reviewing the updated IRM 10.8.1, ESAT office procedures, and National Institute of Standards and Technology guidelines; comparing the updated IRM 10.8.1 and ESAT office procedures to National Institute of Standards and Technology guidelines and the other previously listed guidelines; and ensuring that the updated IRM 10.8.1 included language from the obsolete IRM 10.8.3, *Information Technology (IT) Security, Audit Logging Security Controls*, requiring applications to log/capture any interaction with taxpayer data.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; audit trail information for 31 applications was not being sent to the SAAS (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We collaborated and worked with TIGTA OI and the IRS and determined there are 67 applications that store or process taxpayer data and PII that should be capturing and sending audit trails to the SAAS for unauthorized access monitoring. We reviewed the SAAS and found that 31 (46 percent) of the 67 applications were not sending audit trail information to the SAAS. Because the audit trails for the 31 applications are not available in the SAAS, the IRS cannot ensure that it or TIGTA OI can sufficiently investigate security violations or unauthorized accesses by employees and contractors on all applications where taxpayer data or PII reside.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 28 applications that are required to provide audit trail information to the SAAS were not included in the IRS inventory of all applications that store or process taxpayer data and PII (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We obtained different inventory lists from different offices at different points of the audit. For example, in March 2019, we received an inventory list of 155 applications from the ESAT office, and then a month later, we received another inventory list of 167 applications from business units across the IRS. The final inventory list we received in November 2019 contained 48 applications from the Privacy, Governmental Liaison, and Disclosure office. Throughout the audit, TIGTA OI also provided us with the inventory of applications with which it was working.

We collaborated and worked with TIGTA OI and the IRS and determined there are 67 applications that store or process taxpayer data and PII that should be capturing and sending audit trail information to the SAAS for unauthorized access monitoring. The 67 included 28 (42 percent) applications that were on TIGTA OI's inventory but not on the IRS's inventory list.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger Digitally signed by Nancy A. Sieger Date: 2020.07.06 18:19:11 -0400'
Acting, Chief Information Officer

SUBJECT: Draft Audit Report – Most IRS Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information (Audit # 201920006) (e-trak #2020-23606)

Thank you for the opportunity to review your draft audit report and to discuss the observations with the IRS IT Cybersecurity leadership.

We have an unwavering commitment to the protection of taxpayer data and leverage a number of tools and capabilities to ensure we have a multifaceted approach. UNAX is an important component of the Internal Revenue Service (IRS) auditing program with the goal of improving capabilities to capture auditable events from applications that manage, store, or transact Federal Tax Information (FTI). As noted in the report, IRS has made progress in implementing solutions to address weaknesses. We continue to leverage the IRS Integrated Modernization Business Plan, particularly the Next Generation Enterprise Security Audit Trails initiative to deliver quantifiable improvements. For example, we have leveraged the modernized audit trail solution in specific use cases, which has resulted in a more than a ten-fold reduction in the cycle time for audit log collection, data integration, and report generation, and we will continue to make progress in the years ahead. These enhancements, to be delivered in three phases, will help to further improve analytics and compliance.

The report also acknowledges progress on the UNAX technical solution. We are encouraged by your acknowledgement of our progress and will continue the work to meet IRS, Departmental and Department of Homeland Security (DHS) goals.

As an agency, we are fully invested in the continuous improvement of our oversight and protection of FTI. We are aggressively transforming and automating our existing processes and technologies supporting the UNAX Program. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Richard Therrien at (240) 613-5262.

Attachment

Attachment

Draft Audit Report - Most IRS Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information (Audit #201920006)

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

CORRECTIVE ACTION #1: The IRS partially agrees. Cybersecurity will partner with Privacy, Government Liaison and Disclosure to review and revise the current Privacy Impact Management System to clearly identify applications that store, process or transact Federal Tax Information for the purpose of detecting improper cyber activities and to reconstruct events for potential criminal investigations. This inventory will be updated, at a minimum, annually. The IRS will be replacing the Security Audit and Analysis System (SAAS), however, audit trails records will continue to be tracked in a centralized system.

IMPLEMENTATION DATE: September 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Recommendation 2: The Chief Information Officer should obtain the list of 13 applications with an ACRs that references the obsolete IRM, conduct a revalidation of the auditable events, and issue an AU Deficiency Memorandum to the application owner, if needed, to require an ACR update to comply with the current list of auditable events. In addition, ensure that revalidations are conducted annually as required.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will obtain the list of 13 applications with Audit Control Reponses (ACR) that reference the obsolete Internal Revenue Manual (IRM), correct the reference to reflect current policy, conduct revalidations against the current list of auditable events, and issue Audit Trail (AU) Deficiency Memos to application owners. If changes to the audit trails are identified, then an ACR revalidation is conducted annually as required.

IMPLEMENTATION DATE: October 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report - Most IRS Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information (Audit #201920006)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Recommendation 3: The Chief Information Officer should ensure that application audit trail deficiencies are properly tracked on a POA&M, thus ensuring compliance with the FISMA, IRM policy, and the Office of Management and Budget annual guidance.

CORRECTIVE ACTION #3: IRS agrees with this recommendation. Cybersecurity will ensure that currently identified application audit trail deficiencies are properly tracked in a Plan of Action and Milestones (POA&M) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), Internal Revenue Manual (IRM) policy, and the Office of Management and Budget (OMB) annual guidance.

IMPLEMENTATION DATE: February 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Recommendation 4: The Chief Information Officer should ensure that the IRM policy and the AU Deficiency Memorandum template document clearly and consistently communicates each stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the POA&M is reflective of the issues indicated in the AU Deficiency Memo within 60 calendar days.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Policy is in place and compliant with National Institute of Standards and Technology (NIST) and Treasury Audit Trail (AU) controls. The AU Deficiency Memo template will be revised to clearly and consistently communicate stakeholder's responsibilities to ensure that the appropriate actions are taken, records are properly updated, and the narrative in the Plan of Action and Milestones (POA&M) is reflective of the issues indicated in the AU Deficiency Memorandum within 60 calendar days.

IMPLEMENTATION DATE: February 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Attachment

Draft Audit Report - Most IRS Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information (Audit #201920006)

Recommendation 5: The Chief Information Officer should establish a process improvement so application owners timely create the POA&Ms when audit trail deficiencies are identified. This recommendation also addresses a similar repeat finding from the Fiscal Year 2015 audit report previously mentioned.

CORRECTIVE ACTION #5: IRS agrees with this recommendation. Cybersecurity will document within the Plan of Action and Milestones (POA&M) Standard Operating Procedures (SOP) process improvements to require that application owners create POA&Ms timely when audit trail deficiencies are identified.

IMPLEMENTATION DATE: February 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

Appendix IV

Glossary of Terms

Term	Definition
Audit Control Response	Addresses security auditing for the application and its infrastructure to include the operating system, database, and middleware products. Infrastructure audit configurations are also documented in the ACR. In conjunction with the System Security Plan, the ACR is the ESAT office's official source for documentation of the National Institute of Standards and Technology Special Publication 800-53 auditing controls.
Audit Trail	A chronological record of system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Audit Trail Deficiency Memorandum	A memorandum that notifies the application authorizing official or owner of the auditing deficiencies determined by the Cybersecurity function ESAT office Audit Plan Team and the actions that need to be taken.
Business Unit	A title for major IRS organizations such as Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the Information Technology organization.
Calendar Year	The 12-consecutive-month period ending on December 31.
Cybersecurity Function	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Deficiencies	Audit requirements that have not been met.
Federal Information Processing Standards Publication 199	Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Federal Information System Modernization Act of 2014 Cycle	A yearly cycle from July 1st to June 30th of the following year.
Interface Control Document	Maps the fields in a database/system regarding where and how to access them, so they can be transmitted into the SAAS.

Term	Definition
Material Weakness	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."
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date, place of birth, and mother's maiden name.
Plan of Action and Milestones	A corrective action plan to identify and document the resolution of information security weaknesses and periodically report to the Office of Management and Budget, the Department of the Treasury, and to Congress.
Privacy Impact Assessment	A set of questions that help define how a system affects taxpayers' or employees' privacy and provides a means to assure compliance with applicable laws and regulations governing privacy. A Privacy Impact Assessment is required to be performed and updated every three years or when a major system change creates new privacy risks.
Security Audit and Analysis System	This system implements a data warehousing solution to provide online analytical processing of audit trail data.
Security Controls Assessment	The testing and evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Significant Deficiency	The Department of the Treasury has defined a significant deficiency as 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.
Splunk	This network traffic, database, and analytics tool is an industry standard technology that is used to analyze the streams of machine data generated by information technology systems and technology infrastructure in order to improve both insider threat detection and application troubleshooting.
System Security Plan	Provides an overview of the security requirements for the information system and describes the security controls in place or planned to meet those requirements.
Unified Work Request	Provides the detailed business requirements for data requests so the IRS can properly review, assign, analyze, and respond (approve/deny) to the request, and can also cost and schedule the request for the implementation and delivery of any agreed-upon information technology products or services.

Appendix V

Abbreviations

ACR	Audit Control Response
AU	Audit Trail
EFS	Enterprise Federal Information Security Modernization Act Services
ESAT	Enterprise Security Audit Trails
FISMA	Federal Information Security Modernization Act of 2014
ICD	Interface Control Document
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OI	Office of Investigations
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SAAS	Security Audit and Analysis System
TIGTA	Treasury Inspector General for Tax Administration