TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls

September 21, 2023

Report Number: 2023-20-064

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

HIGHLIGHTS: Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls

Final Audit Report issued on September 21, 2023 **Report Number 2023-20-064**

Why TIGTA Did This Audit

The Cyber Security Assessment and Management application (CSAM) is developed and maintained by the U.S. Department of Justice. The IRS leverages the CSAM to complete the National Institute of Standards and Technology, Special Publication 800-53, security control assessments and to maintain system security plans throughout the systems' lifecycle.

This audit was initiated to determine whether the IRS is effectively implementing the CSAM.

Impact on Tax Administration

The CSAM provides IRS program and information assurance officials the capability to assess, document, manage, and report on the status of information technology. The CSAM will allow the IRS to maintain real-time updates to system security plans. According to the National Institute of Standards and Technology, the objective of system security planning is to improve protection of information system resources, *i.e.*, protect taxpayer information and information systems.

What TIGTA Found

TIGTA determined that on-premise reportable systems were tracked in the CSAM. TIGTA did not include an inventory review of cloud systems because the IRS was conducting a proof of concept on a sample of cloud systems.

Improvements can be made reviewing the CSAM audit logs to identify suspicious activities. TIGTA requested user audit log summary reports from September through November 2022, and the IRS could not provide seven (54 percent) reports over the 13-week period. The IRS was also unable to provide documented evidence it reviewed the user audit log summary reports. In addition, the separation of duties principle was not enforced, as CSAM system administrators are reviewing their own audit logs.

Nine (3 percent) of 328 active CSAM users were not authorized to access the application. During our audit work, the IRS provided authorizations for all nine users. In addition, TIGTA identified that 308 (36 percent) of 863 active and inactive CSAM users had not logged on to the application for 366 to 1,205 calendar days. The users were not removed from the system as required by policy because removing the users would remove any audit logs associated with the accounts. However, no risk-based decision was created for the exception to policy.

To test the accuracy and completeness of the system security plans, TIGTA reviewed security documents of five systems and identified 32 controls with weaknesses. The five system security plans did not capture remedial information to address the identified weaknesses.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer 1) ensure that the CSAM audit logs are reviewed weekly and the results of review are documented; 2) ensure that the CSAM system security plan is updated to include clarification for security specialists to review audit logs; 3) create a risk-based decision accepting the risk for allowing accounts to remain on the CSAM after 365 days of inactivity; and 4) coordinate with system owners to ensure that Plans of Action and Milestones with identified weaknesses are updated in the system security plans.

The IRS agreed with two recommendations and stated that weekly audit log reviews are documented and archived, and the Information System Security Officer is included in the weekly review of audit logs. The IRS stated that it has processes in place for the two remaining recommendations and requested that TIGTA consider them resolved.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 21, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls (Audit # 202320005)

This report presents the results of our review to determine whether the Internal Revenue Service is effectively implementing the Cyber Security Assessment and Management application. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources.*

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

Table of Contents

Background

The Federal Information Security Modernization Act of 2014 (FISMA) focuses on improving oversight of the Federal information security program and facilitating progress in correcting agency information security weakness.[1] It requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. A key component of FISMA is the automated processes of Information Security Continuous Monitoring. In support of Information Security Continuous Monitoring, the Internal Revenue Service (IRS) uses the Cyber Security Assessment and Management application (hereafter referred to as CSAM).

CSAM is developed and maintained by the U.S. Department of Justice (DOJ). The IRS leverages CSAM to complete National Institute of Standards and Technology (NIST) Special Publication security control assessments and to maintain system security plans (SSP) throughout the systems' lifecycle.[2] The CSAM also provides an agencywide view of the status of information system security, the implementation of information technology security controls, and information system compliance documentation. In addition, the CSAM provides IRS program and information assurance officials the capability to assess, document, manage, and report on the status of information technology.

The DOJ owns the CSAM and provides IRS users with access to the application. The IRS Cybersecurity FISMA Certification Program Office implemented the CSAM in Fiscal Year 2020 with the goal of moving security controls assessments to a more automated process. The DOJ is responsible for CSAM operations and maintenance activities. IRS users have access to system security controls assessment data maintained on the CSAM database via a secure website. The IRS pays an annual fee for use of the application and support activities.

The IRS uses a three-year control assessment cycle, *i.e.*, generally one third of controls are assessed every year with all controls assessed during a three-year period.[3] In Fiscal Year 2020, the IRS piloted the CSAM on two FISMA systems. The success of this pilot enabled the IRS to generate assessment plans; collect evidence for the assessment within the CSAM; complete applicable NIST, Special Publication 800-53, security controls; and generate SSPs. Full implementation of the CSAM for all annual security controls assessments for the first one third of controls began in FISMA Year 2021, the first full three-year cycle was planned to be completed in FISMA Year 2023.

However, during the Fiscal Year 2022 FISMA evaluation, the IRS explained that it transitioned from NIST, Special Publication 800-53 Rev. 4 to Rev. 5.[4] Therefore, it will fully complete all

[1] Pub. L. No. 113-283. See Appendix III for a glossary of terms.

[2] NIST, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

[3] Some controls are assessed annually, such as Critical/Volatile controls.

[4] NIST, Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

control assessments based on NIST, Special Publication 800-53 Rev. 5, controls in FISMA Year 2024, *i.e.*, by July 2024.

Results of Review

All On-Premise Systems Were Tracked in the Cyber Security Assessment and Management Application

We determined that all on-premise FISMA reportable systems were tracked in the CSAM, an IRS official repository of information systems. According to the CSAM Standard Operating Procedure, the CSAM team must perform a yearly reconciliation to ensure that the inventory within the CSAM aligns with the current stated FISMA boundaries as outlined in the FISMA Master Inventory.

We obtained and reconciled a list of systems tracked by CSAM and a list of FISMA reportable systems from the Treasury FISMA Inventory Management System (TFIMS) as of January 26, 2023. The CSAM had 129 on-premise systems. We identified a discrepancy that was not identified during the last inventory validations performed by the CSAM team. After we informed the CSAM team of our results, they determined that the system in question was accidently not categorized as a FISMA reportable system and provided evidence to show that the discrepancy was corrected.

For our analysis, we did not include an inventory review of cloud systems because the IRS was conducting a proof of concept on a sample of cloud systems to determine the feasibility of using CSAM to support cloud security documents. The IRS stated that it has not determined whether to transition cloud security documents to the CSAM, because it plans to transition from the CSAM to a Treasury-approved Information Technology Service Management cloud-based platform by June 2024.

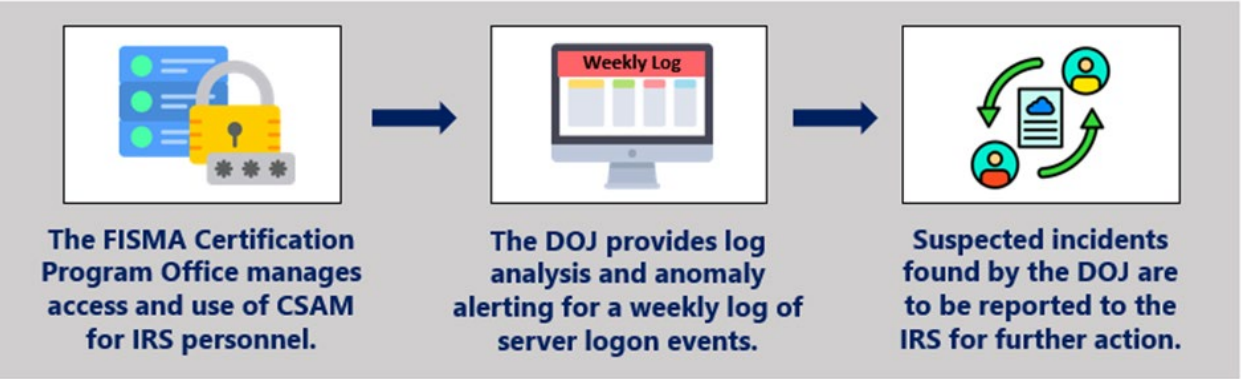
Cyber Security Assessment and Management Application Security Controls Are Not Effectively Implemented

Based on the DOJ Control Implementation Summary Control Matrix, the Interconnection Security Agreement between the IRS and the DOJ, the Internal Revenue Manual (IRM), and NIST, Special Publication 800-53 Rev. 5, the IRS has not effectively implemented audit logs, separation of duties, and account management security controls.[5]

[5] *Interconnection Security Agreement Between U.S. Internal Revenue Service and U.S. Department of Justice* (Nov. 2020), IRM 10.8.1, *Information Technology (IT) Security, Policy, and Guidance* (Dec. 2022), and IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* (Sept. 2022).

Improvements can be made reviewing the CSAM audit logs to identify suspicious activities

The Cybersecurity function's FISMA Certification Program Office manages the access and usage of the CSAM for IRS personnel. The DOJ aggregates the CSAM audit record using the DOJ's security information and event management system which provides log analysis and anomaly alerting capabilities to support a weekly audit log review focused on server logon events. Any suspected incidents identified in the weekly audit record report during the DOJ's reviews are to be reported to the IRS for research and follow-up.



The IRS receives user audit log summary reports from the DOJ. This report consists of failed logon attempts summarized by aggregating total failed attempts per user. For these reports, the DOJ requests the IRS to review failed logon attempts and respond confirming the activity was legitimate or advise if any activity is indeed suspicious. As of May 31, 2023, aside from failed logons, the IRS stated that it has not had any suspicious activities since the CSAM was implemented in July 2020.

The IRS lacks evidence to show it reviews audit logs weekly for suspicious activity

We requested user audit log summary reports from September through November 2022 and the IRS could not provide seven (54 percent) reports out of the 13 weeks. Further, the IRS did not provide any evidence that written responses were provided to the DOJ regarding the IRS review of the audit log summary reports. The IRS stated it meets weekly with the DOJ and communicates any CSAM issues; however, the IRS did not have any official agendas or minutes of these meetings. The CSAM SSP states the CSAM main administrator reviews and analyzes weekly the CSAM audit records, as they relate to account management, for indications of inappropriate or unusual activity. In addition, IRM 10.8.2 states audit logs should be reviewed weekly to detect inappropriate user and system actions that could be construed as security incidents.

We reviewed and compared one of the six user audit log summary reports that the IRS received from the DOJ to the actual CSAM user application logs to determine if the summary of user failed logon attempts matched the actual failed logon attempts. The user audit log summary report had six users with failed logon attempts ranging from three to seven failed attempts.

Our review found discrepancies with two (33 percent) of the six users after comparing the audit log summary reports to the CSAM user application logs. Specifically,

- In one case, the access date reported on the audit log summary report did not match the actual CSAM user application log.

- In one case, the audit log summary report showed only seven logon attempts, while the CSAM user application log showed the user made eight attempts.

The IRS stated that it will need to ask the DOJ for a reason why the date of access and the count of failed logons did not match the actual audit log. As of August 2, 2023, the IRS has not provided a response to explain the discrepancies.

The DOJ Control Implementation Summary Control Matrix states that CSAM customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined personnel or roles in accordance with their audit and accountability policy. Monitoring system accounts for atypical usage includes, accessing systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations and reporting atypical usage of system accounts to organization-defined personnel or roles.

Due to the IRS's inability to provide documented evidence to support it reviews logs and the missing weekly audit log summary reports, we concluded that the IRS is not reviewing the audit logs for suspicious activity on a weekly basis. The IRS cannot fully determine whether documented events are legitimate and not suspicious without reviewing the audit logs.

Recommendation 1: The Chief Information Officer should ensure that the CSAM audit logs are reviewed weekly and the results of the review are documented.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer is ensuring the weekly audit log reviews for suspicious activity are documented and archived. The IRS initiated this practice in July 2023.

Office of Audit Comment: The IRS stated it initiated this practice at the end of our audit work. Therefore, we did not verify that the IRS is reviewing the CSAM audit logs weekly and documenting its review.

Lack of separation of duties in reviewing CSAM audit logs

While the lack of weekly reviews of the CSAM audit logs is an issue, we also found that the separation of duties principle was not enforced when CSAM audit logs were reviewed. Specifically, CSAM system administrators with administrator privileges are reviewing their own audit logs. In addition, we determined the CSAM SSP does not align with IRM requirements. The SSP stated that the CSAM main administrator shall review and analyze CSAM audit records weekly as they relate to account management for indications of inappropriate or unusual activity. However, the IRM states that the security specialist shall review all types of audit logs/trails and observe system activity at least weekly. The IRS stated that the DOJ Control Implementation Summary Control Matrix directs the system administrators to review audit logs; however, in our review, we determined that the control matrix is not specific on who should review the audit logs.

NIST, Special Publication 800-53 Rev. 5, states separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

The IRS stated that they allow CSAM administrators to review audit logs because system administrators are categorized as security specialists. Also, the DOJ Information System Security Officer reviews all CSAM audit logs, and a report of suspicious activity is generated for IRS administrators to investigate. We disagree with the IRS's position. Although CSAM system administrators are categorized as security specialists, these employees are conducting system administrator's duties in administering, maintaining, and operating the CSAM which allows administrators to create users and enable or disable access to the CSAM.

The separation of roles and responsibilities ensures that no one person has the authority or ability to circumvent checks and balances. Enacting this control prevents the potential misuse of administrator privileges in reviewing the system logs or audit reports that could alert an independent reviewer of potential system misuse.

Recommendation 2: The Chief Information Officer should ensure that the CSAM SSP is updated to include clarification for security specialists to review audit logs to comply with the NIST, Special Publication 800-53 Rev. 5, separation of duties control.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer is ensuring that the CSAM SSP is updated to clarify who is responsible for reviewing and investigating audit logs. In July 2023, the IRS initiated the practice of including the CSAM Information System Security Officer in the weekly review of audit logs for suspicious activity. This practice ensures the Information System Security Officer maintains visibility into potentially suspicious activity in accordance with the applicable NIST requirements and institutes a control for the separation of duties.

Office of Audit Comment: The IRS stated it initiated this practice at the end of our audit work. Therefore, we did not verify that the CSAM SSP was updated in accordance with the NIST guidance and that the CSAM Information System Security Officer is reviewing audit logs for suspicious activity.

The CSAM account management security controls need improvement

As previously stated, the Cybersecurity function's FISMA Certification Program Office manages the access and usage of the CSAM for IRS personnel. Based on our discussions with the IRS, the process to obtain CSAM access requires the user to request access through the Business Entitlement Access Request System (BEARS), take the CSAM training course, and create an account in the CSAM. To determine if the CSAM has appropriate access management controls in place for unauthorized users, we obtained user entitlement data from BEARS and a list of users from the CSAM.

- The BEARS data had a list of 582 production users with authorization to access the CSAM as of January 25, 2023.
- The CSAM data had a list of 328 active users as of January 30, 2023.

Our review and comparison of the lists determined the following:

CSAM users did not have proper authorization for CSAM access

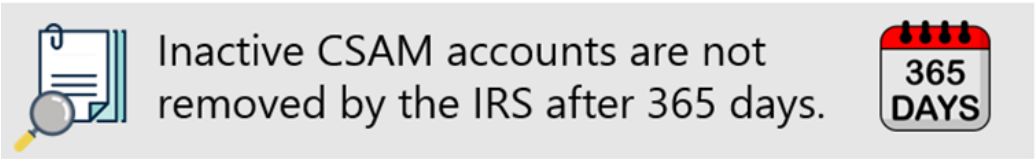
We compared the 328 CSAM active users to the 582 CSAM authorizations in BEARS and determined that nine (3 percent) of the 328 active users were not authorized in BEARS. The Interconnection Security Agreement between the IRS and the DOJ states that the IRS is responsible for the account management lifecycle for all its user community (account creation, profiling, modification, deletion, recertification, *etc.*). In addition, IRM 10.8.1 requires that the Service-wide process, the BEARS, be used to register all users requiring access to any IRS information technology resource.

For the nine CSAM users, the IRS conducted research to determine reasons why users were authorized to have access to CSAM without BEARS approval. The IRS stated that except for one user, the migration of user account data from the Online 5081 system to the BEARS could have contributed to this finding. For the one user, the IRS stated that there was a pending approval request and the system's administrator created the account prior to the account's full approval.

Management Action: After we informed management of our results, the IRS CSAM system administrators approved one pending user request and asked the remaining eight users to initiate and process BEARS requests. We subsequently verified that a BEARS authorization was approved for the nine users.

Risk-based decision was not created for an exception to policy

We obtained a list of 863 active and inactive CSAM user accounts from the IRS on February 22, 2023, to determine whether the IRS was monitoring user activity and appropriately removing inactive users. We found 308 (36 percent) of the 863 CSAM users had not logged on for over 365 days. The calendar days for inactive accounts ranged from 366 to 1,205 days.



IRM 10.8.1 requires user accounts be removed after 365 calendar days of inactivity. The IRS and DOJ stated that accounts are not deleted in the CSAM because deleting an account would remove any audit logs associated with the specific account. We agree that maintaining audit log traceability is preferable to account deletion and found that the IRS has mitigating controls in place by locking all 308 user accounts from accessing the CSAM. However, the IRS does not have a risk-based decision documented to accept the risk for this exception to policy. IRM 10.8.1 states that any exception to policy requires the authorizing official to make a risk-based decision.

Access controls limit access to information and information processing systems. When implemented effectively, they mitigate the risk of information being accessed without the appropriate authorization or unlawfully and the risk of a data breach. The IRS increases the

amount of risk and exposure pertaining to potential unauthorized accesses and disclosure of information by not addressing weaknesses in its access management controls.

Recommendation 3: The Chief Information Officer should create a risk-based decision accepting the risk for allowing accounts to remain on the CSAM after 365 days of inactivity.

Management's Response: The IRS stated that it has processes in place and requested that the Treasury Inspector General for Tax Administration (TIGTA) consider this recommendation resolved and closed, as implemented. The Chief Information Officer has verified that inactive accounts on the CSAM pose no risk to the data or to the IRS. The current practice automatically locks accounts after 90 days of inactivity. A risk-based decision is not required because inactive accounts pose no risk.

Office of Audit Comment: We disagree that inactive accounts on the CSAM do not pose any risk to the data or to the IRS. Compensating controls may mitigate the risk of indefinitely keeping inactive accounts on the CSAM, but they do not eliminate risks to the data or to the IRS. Not deleting accounts after 365 days of inactivity is an exception to the policy within the IRM, and the IRM requires the authorizing official to document a risk-based decision for any exception to policy.

System Security Plans Were Not Always Updated to Accurately Reflect Remedial Information for Controls With Identified Weaknesses

We selected five sampled systems from the 2023 FISMA annual security controls assessment and traced the control deficiencies from the 2023 FISMA annual assessment plans to the Security Assessment Report and then to the SSP.[6] We identified 32 controls in the SSPs that were not updated to reflect remedial information.

The CSAM is used to reflect the status of controls with a real-time update to SSPs. Although the SSPs had the correct status of controls in four (80 percent) of the five systems, all five systems were lacking Plans of Action and Milestones (POA&M) information on the deficiencies of the controls as shown in Figure 1.

[6] To test the accuracy and completeness of control assessment information and system security information in the CSAM, we selected a judgmental sample of five systems by leveraging the sample selection process from the Fiscal Year 2023 FISMA evaluation. TIGTA, Report No. 2023-20-041, *Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation* (Aug. 2023). The five systems should cover security controls recommended for evaluation for year 1, year 2, and year 3 testing. A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Figure 1: Remedial Information to Mitigate Control Weaknesses Not Updated in the SSPs

System	Weaknesses identified in the Annual Assessment Plan	Weaknesses documented in the Security Assessment Report or had an open POA&M	Weaknesses documented in the SSP - Status of Control	SSPs not updated to accurately reflect remedial information
System 1	11	11	11	3
System 2	6	6	6	4
System 3	6	6	6	3
System 4	38	38	36	9
System 5	19	19	19	13
Total				**32**

Source: TIGTA's analysis of the five sampled FISMA systems.

All Federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in an SSP. According to NIST, Special Publication 800-18 Rev. 1, the objective of system security planning is to improve protection of information system resources, *i.e.*, protect taxpayer information and information systems, and the purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls in place or plans to meet those requirements.[7] NIST, Special Publication 800-18 Rev. 1, also states that SSPs require periodic review and modification and POA&Ms for implementing security controls.

Security Risk Management officials stated that requiring the manual entry of assessment results and POA&M information into the SSP would defeat the purpose of automating the Risk Management Framework process and would create a condition that requires a high level of effort to maintain with little value along with the duplication of information which can quickly and easily become inconsistent. In addition, updating the SSP is the responsibility of the stakeholders. If the POA&M information is not in the SSP, it is because the appropriate stakeholder did not add it. The IRS stated that the remedial actions are documented in TFIMS for POA&Ms and a commercial off-the-shelf product for risk-based decisions. We determined that the CSAM FISMA assessors do not have access to the TFIMS where the POA&Ms are tracked and maintained; therefore, the system stakeholders would need to update the POA&M information in the SSPs.

We determined that the POA&M information should be in the SSP as it documents plans to meet requirements for necessary controls not implemented. Without the POA&M information being documented within the SSP, the SSP becomes a less effective tool to summarize the security requirements for the information system and describe the security controls in place or plans for meeting those requirements.

[7] NIST, Special Publication 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (Feb. 2006).

Recommendation 4: The Chief Information Officer should coordinate with system owners to ensure that POA&Ms with identified weaknesses are updated in the SSPs.

Management's Response: The IRS stated that it has processes in place and requested that TIGTA consider this recommendation resolved and closed, as implemented. The Chief Information Officer documents the POA&Ms to address identified security weaknesses using authoritative data sources. The processes the IRS has in place ensures documentation of all remedial actions to track control deficiencies identified during security control assessments. There is no requirement that the SSPs be the exclusive source for documenting remedial actions. The IRS documents POA&Ms using alternative and authoritative data sources in accordance with requirements set forth by the NIST and the IRM. Specifically, the IRS uses the TFIMS to document POA&Ms and it uses a system called Archer to document risk-based decisions.

Office of Audit Comment: We disagree that the IRS adheres to NIST requirements. According to NIST, plans to meet security control requirements should be documented in the SSP. Without the POA&M information, the SSP becomes a less effective tool at providing an overview of the security posture and weakness that must be addressed.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the IRS is effectively implementing the CSAM. To accomplish our objective, we:

- Reviewed Federal Government and IRS requirements for maintaining a current and accurate inventory of systems, conducting annual FISMA control security assessments, maintaining separation of duties, and reviewing audit logs.
- Determined whether CSAM contains an accurate system inventory by ensuring that all FISMA reportable systems are tracked to ensure that they undergo the required annual security controls assessment. We compared the TFIMS system inventory list with a CSAM inventory list dated January 26, 2023.
- Determined whether the IRS independently analyzed CSAM audit logs for suspicious activities by interviewing DOJ and IRS personnel regarding the CSAM audit log review process. We also reviewed audit log referrals the DOJ provided to the IRS from September through November 2022.
- Determined if the CSAM has appropriate access management controls in place for user accounts by interviewing DOJ and IRS personnel to determine how CSAM is accessed. We also reviewed and compared the list of CSAM users in the BEARS to a list of CSAM users obtained from IRS administrators to verify users' authorization and activity.
- Determined if the SSPs are reporting accurate security controls assessment results by reviewing and tracing weaknesses from the Assessment Plan to the Security Assessment Report and then to the SSPs for five systems. We determined if the control status was properly documented and if vulnerability information has been omitted by comparing the weaknesses in each document. We interviewed IRS personnel to discuss the discrepancies. A judgmental sample of five systems was selected from the Fiscal Year 2023 FISMA evaluation, which had a sample population of seven systems.[1] We selected a judgmental sample because we did not plan to project to the population.

Performance of This Review

This review was performed with information obtained from the Security Risk Management office located in Martinsburg, West Virginia, during the period November 2022 through July 2023. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[1] TIGTA, Report No. 2023-20-041, *Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation* (Aug. 2023). A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Midori Ohno, Audit Manager; Ashley Weaver, Lead Auditor; and Cari Fogle, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

During this review, we relied on data received from the IRS.

- We performed tests to assess the reliability of the system inventory data obtained from the TFIMS website. We evaluated the data by 1) ensuring that the information was legible and contained alphanumeric characters; 2) reviewing required data elements; and 3) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined the data were sufficiently reliable for the purpose of the report.
- We performed tests to assess the reliability of the list of systems and users from the CSAM. We evaluated the data by 1) interviewing the IRS about the data; 2) reviewing information about the data and the CSAM; 3) reviewing user account information such as names and e-mail addresses; and 4) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined that the data were sufficiently reliable for the purposes of the report.
- We performed tests to access the reliability of the list of systems from BEARS. We evaluated the data by 1) ensuring that the information was legible and contained alphanumeric characters; 2) reviewing required data elements; 3) reviewing user account information such as names and e-mail addresses; and 4) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined the data were sufficiently reliable for the purpose of the report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRS policies and procedures related to information technology security, NIST guidance, and Office of Management and Budget guidance. We evaluated these controls by interviewing IRS management and staff, reviewing data and artifacts from applicable systems, and reviewing program documentation.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 11, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Acting Chief Information Officer

Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2023.09.11 11:32:43 -04'00'

SUBJECT: Draft Audit Report – Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls (Audit # 202320005)

Thank you for the opportunity to review and comment on the draft audit report. The Cyber Security Assessment and Management Application (CSAM) is one of several tools we use to maintain the security of our systems and the taxpayer information they contain, and we appreciate recommendations to further improve our security controls.

As noted in the report, CSAM is developed and maintained by the U.S. Department of Justice. The application enables the IRS to assess, document, manage, and report on the security status of information technology assets. We have used the application since July 2020 and have procedures in place to review failed logon attempts, confirm the legitimacy of reported activities and advise if any activity is indeed suspicious. As of May 31, 2023, aside from failed logons, the IRS has not had any suspicious activities to report.

Generally, we agree with the audit team's recommendations to further improve our documentation practices and adherence to procedure. Regarding the first recommendation, our standard practice is to review the CSAM audit logs weekly for suspicious activity, as required. However, we recognize the benefits of documenting the results of each review for quality assurance purposes, and we agree to the recommendation. We also agree with the second recommendation to clarify how we ensure separation of duties, which prevents any one person from having the authority or ability to circumvent checks and balances. We agree with these first two recommendations and have already implemented them, therefore no corrective action plans are required.

The third recommendation focuses on how the IRS handles inactive CSAM accounts. As noted in the report, the Treasury Inspector General for Tax Administration (TIGTA) agrees that maintaining audit log traceability is preferable to account deletion. TIGTA

also found that the IRS has mitigating controls in place by automatically locking inactive accounts from accessing the CSAM. A risk-based decision is not required because inactive accounts do not create any risk, and therefore we request that TIGTA consider the third recommendation resolved and closed, as implemented.

The fourth recommendation relates to enhancing system security plans (SSPs). According to the National Institute of Standards and Technology (NIST), the purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls in place or plans to meet those requirements. The IRS fully adheres to this NIST requirement. The Chief Information Officer currently has a process in place that ensures documentation in the authoritative sources for remedial actions, and we request that TIGTA consider the fourth recommendation resolved and closed, as implemented.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-5000, or a member of your staff may contact Caralee Garr, director of Security Risk Management, at 801-620-4140.

Attachment

Attachment

RECOMMENDATION 1:
The Chief Information Officer should ensure that the CSAM audit logs are reviewed weekly and the results of the review are documented.

CORRECTIVE ACTION:
The Chief Information Officer (CIO) is ensuring the weekly audit log reviews for suspicious activity are documented and archived. We initiated this practice in July 2023.

IMPLEMENTATION DATE:
N/A

RESPONSIBLE OFFICIAL(S):
N/A

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION 2:
The Chief Information Officer should ensure that the CSAM SSP is updated to include clarification for security specialists to review audit logs to comply with the NIST, Special Publication 800-53 Rev. 5, separation of duties control.

CORRECTIVE ACTION:
The CIO is ensuring that the CSAM SSP is updated to clarify who is responsible for reviewing and investigating audit logs. We have already taken actions to address this recommendation. In July 2023, we initiated the practice of including the CSAM Information System Security Officer (ISSO) in the weekly review of audit logs for suspicious activity. This practice ensures the ISSO maintains visibility into potentially suspicious activity in accordance with the applicable NIST requirements and institutes a control for the separation of duties.

IMPLEMENTATION DATE:
N/A

RESPONSIBLE OFFICIAL(S):
N/A

CORRECTIVE ACTION MONITORING PLAN:
N/A

Attachment

RECOMMENDATION 3:
The Chief Information Officer should create a risk-based decision accepting the risk for allowing accounts to remain on the CSAM after 365 days of inactivity.

CORRECTIVE ACTION:
The CIO has verified that inactive accounts on the CSAM pose no risk to the data or to the IRS. The current practice automatically locks accounts after 90 days of inactivity. A risk-based decision is not required because inactive accounts pose no risk. We request TIGTA consider this recommendation resolved and closed, as implemented.

IMPLEMENTATION DATE:
N/A

RESPONSIBLE OFFICIAL(S):
N/A

CORRECTIVE ACTION MONITORING PLAN:
N/A

RECOMMENDATION 4:
The Chief Information Officer should coordinate with system owners to ensure that POA&Ms with identified weaknesses are updated in the SSPs.

CORRECTIVE ACTION:
The CIO documents the plan of action and milestones (POA&Ms) to address identified security weaknesses using authoritative data sources. The processes we have in place ensure documentation of all remedial actions to track control deficiencies identified during security control assessments. There is no requirement that SSPs be the exclusive source for documenting remedial actions. We document POA&Ms using alternative and authoritative data sources in accordance with requirements set forth by the National Institute of Standards and Technology and the Internal Revenue Manual. Specifically, we use the Treasury FISMA Inventory Management System (TFIMS) to document POA&Ms and we use a system called Archer to document risk-based decisions. Because the IRS documents remedial actions within these authoritative sources, we request TIGTA consider this recommendation resolved and closed, as implemented.

IMPLEMENTATION DATE:
N/A

RESPONSIBLE OFFICIAL(S):
N/A

CORRECTIVE ACTION MONITORING PLAN:
N/A

Appendix III

Glossary of Terms

Term	Definition
Access Controls	A policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: 1) passing the information to unauthorized subjects or objects; 2) granting its privileges to other subjects; 3) changing one or more security attributes on subjects, objects, the information system, or system components; 4) choosing the security attributes to be associated with newly created or modified objects; or 5) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges, *i.e.*, they are trusted subjects, such that they are not limited by some or all of the noted constraints.
Application	A software program hosted by an information system.
Audit Log	NIST defines audit log as a chronological record of information system activities, including records of system accesses and operations performed in a given period.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Business Entitlement Access Request System	The IRS's automated tool to support the management of system accounts. BEARS is used to create, enable, modify, disable, and remove accounts and notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred.
Cloud	The use of computing resources, *e.g.*, hardware and software, which are delivered as a service over a network (typically the Internet).
Control/Internal Control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. It comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. It also serves as the first line of defense in safeguarding assets. In short, controls help managers achieve desired results through effective stewardship of public resources.
Cyber Security Assessment and Management Application	Provides an agencywide view of the status of information system security and documented processes, implementation of IRS mandated information technology security controls, and information system compliance documentation.
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.

Term	Definition
Department of Justice Control Implementation Summary Control Matrix	Lists the division of security control responsibilities between the IRS and the DOJ for the CSAM.
Entitlement	Rights granted to the user of licensed software that are defined within the license agreement.
Federal Information Security Modernization Act of 2002	Requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget.
Federal Information Security Modernization Act of 2014	Amendment to the Federal Information Security Management Act of 2002 that allows for further reform to Federal information security, signed 12 years after the passing of the original law. This bill amends Chapter 35 of Title 44 of the United States Code.
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.
FISMA Year	The reportable period for FISMA activities, from July 1 through June 30 of the following year.
Interconnection Security Agreement	An agreement established between the organizations that own and operate connected information technology systems to document the technical requirements of the interconnection.
Internal Revenue Manual	The primary, official source of IRS instructions to staff related to the organization, administration, and operation of the IRS.
Inventory	To take stock of assets. A detailed list of assets.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
Network	An information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
On-Premise	Servers hosted on a network or within a company infrastructure that are controlled, administered, and maintained by the organization.
Online 5081	A web-based system that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The system also allows the IRS to track user access history, generate reports, and document an audit trail of user actions. Online 5081 was replaced by BEARS.

Term	Definition
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Security Assessment Report	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
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.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Treasury FISMA Inventory Management System	A central management tool for cybersecurity activities such as Security Assessment and Authorization and Information Security Continuous Monitoring and is the authoritative source for the Department's FISMA system inventory.

Appendix IV

Abbreviations

BEARS	Business Entitlement Access Request System
CSAM	Cyber Security Assessment and Management Application
DOJ	Department of Justice
FISMA	Federal Information Security Modernization Act of 2014
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SSP	System Security Plan
TFIMS	Treasury FISMA Inventory Management System
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.