TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements

March 27, 2023

Report Number: 2023-20-018

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

HIGHLIGHTS: The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements

Final Audit Report issued on March 27, 2023 **Report Number 2023-20-018**

Why TIGTA Did This Audit

The Enterprise Case Management (ECM) system was one of 41 IRS systems hosted by one cloud service provider as of September 2022. The ECM system is a hybrid cloud system, with components residing on IRS premises and in the cloud. The IRS implemented the first release of the ECM system in December 2020.

TIGTA initiated this audit to evaluate whether the security controls over the ECM system adequately protect its data against unauthorized access.

Impact on Tax Administration

The ECM system is designed to modernize and consolidate legacy case management systems across the IRS. The ECM system processes and stores sensitive information within the IRS, providing restricted access to IRS employees via the Internet. The ECM program's goal is to provide an enterprise solution to perform case management functions using the cloud to reduce long-term costs and increase operational efficiency, innovation, and security.

Control weaknesses within the ECM system can pose a substantial risk to taxpayer records currently residing in the system. The potential harm includes breach, unauthorized access, and disclosure of taxpayer information.

What TIGTA Found

The IRS followed the agency cloud authorization to operate process for the ECM system. However, the IRS did not meet agency guidelines for the timely creation and documentation of Plans of Action and Milestones (POA&M) to address nine security risks identified in the February 2021 Cloud Security Assessment Report. While the IRS created nine POA&Ms, only three (33 percent) were timely prepared and only two (22 percent) met documentation requirements. The IRS took corrective action during the audit to address this finding.

The IRS also tested 42 security controls in June 2022 and identified five risks previously reported in February 2021. TIGTA reviewed the risks and found that actions were taken to address or track the risks including acceptance, remediation, and creating new POA&Ms. In addition, ECM system production servers residing in the cloud lacked required malicious code protection. The IRS did not address the lack of malicious code protection for over a year due to not using the appropriate security policy. During our audit work, the IRS initiated a pilot test of an application to provide malicious code protection for the servers.

The IRS did not timely remediate 24 high- and two medium-risk vulnerabilities for the ECM system, but took actions to mitigate the risks and developed a program-level POA&M. In addition, TIGTA reviewed a configuration compliance report for the ECM system servers and found that all production servers were configured properly.

Finally, ECM system user account management controls are not effective. Specifically, 315 (79 percent) of 401 user accounts were not timely deactivated or disabled, as required. The IRS took corrective action during the audit to deactivate user accounts after 90 calendar days of inactivity. Also, privileged user accounts are not monitored properly.

What TIGTA Recommended

The Chief Information Officer should 1) ensure that Internal Revenue Manuals are consistent with National Institute of Standards and Technology guidelines for malicious code protection requirements for Linux servers; 2) complete development and testing of an automated malicious code protection application and implement the application on all Linux servers; 3) ensure that all ECM servers in the cloud meet malicious code protection requirements; and 4) ensure that privileged user activity logs are monitored and inactive accounts deactivated in accordance with agency requirements.

The IRS agreed with all our recommendations. The IRS plans to update the Internal Revenue Manual; complete development, testing, and implementation of an automated malicious code protection application for Linux servers; and monitor privileged user activity logs and regularly disable inactive privileged accounts.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

March 27, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements (Audit # 202220009)

This report presents the results of our review to evaluate whether the security controls over the Enterprise Case Management system were adequately protecting its data against unauthorized access. 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 [Internal Revenue Service] Resources*.

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

Table of Contents

Appendices

Background

The Enterprise Case Management (ECM) system is designed to modernize and consolidate legacy case management systems, across the Internal Revenue Service (IRS), into an end-to-end enterprise solution in the cloud. The ECM system processes and stores sensitive information, providing restricted access to IRS employees via the Internet. According to the IRS, the ECM program's goal is to provide an enterprise solution to perform case management functions using the cloud to reduce long-term costs and increase operational efficiency, innovation, and security. In December 2020, the IRS implemented the first release of the ECM system.

The ECM system is used for processing and storing sensitive information, providing restricted access to IRS employees via the Internet.

The ECM system is a hybrid cloud system:

2 production servers reside on IRS premises

2 production servers reside in the cloud

As of September 2022, the ECM system was one of 41 IRS systems hosted by one cloud service provider.[1] The ECM system is a hybrid cloud system with components residing on IRS premises (hereafter referred to as on-premise) and in the cloud. The ECM system has two on-premise production servers that are regulated by the IRS's standard Information Technology Security Policy Internal Revenue Manual (IRM) and two production servers in the cloud that are regulated by the IRS Cloud Computing Security Policy IRM.[2] Control weaknesses within the ECM system can pose a substantial risk to taxpayer records currently residing in the system. The potential harm includes breach, unauthorized access, and disclosure of taxpayer information.

Results of Review

Authorization to Operate Process Followed Agency Guidelines

Prior to deploying the ECM system, the Information Technology organization's Cybersecurity function evaluated the implementation status of cloud security controls and issued a Cloud Security Assessment Report documenting the security weaknesses that must be remediated. According to the IRS, security controls for the ECM on-premise servers are evaluated and inherited from the Linux environment and do not require a separate authorization to operate. We reviewed the preliminary Cloud Security Assessment Report, the Enterprise Linux Platform's Security Assessment Report, the System Security Plan, and the Authorization to Operate memorandum and determined that the IRS was compliant with IRM requirements. The IRM

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

[2] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (Sept. 28, 2021) and IRM 10.8.24, *Information Technology Security, Cloud Computing Security Policy* (Sept. 28, 2021).

states that the security authorization process is an inherently Federal responsibility and, therefore, authorizing officials shall be Federal employees. The authorizing official is required to authorize the system to operate before commencing operations.

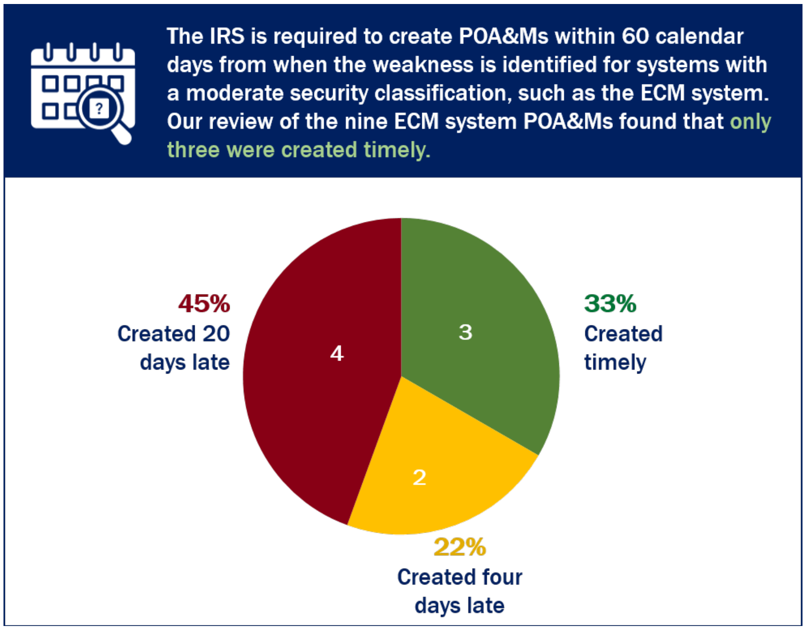
In April 2022, we met with the Cybersecurity function and Enterprise Program Management Office personnel to discuss the certification process that the IRS followed to request an Authority to Operate for the ECM system. Management officials stated that the IRS built the ECM system within an existing cloud that is Federal Risk and Authorization Management Program (FedRAMP) certified. ECM management officials also provided documentation from June 2019 showing that they contacted FedRAMP officials for guidance to ensure that the ECM program met the FedRAMP authorization requirements. FedRAMP officials advised ECM management that the agency authorization process, without FedRAMP involvement, was the appropriate path for authorization.

Plans of Action and Milestones Were Not Timely Prepared and Contained Insufficient Documentation Following the Initial Security Assessment

In February 2021, the Cybersecurity function's Security Risk Management office issued nine system security risks to the ECM Authorizing Official.[3] System owners are required to create a Plan of Action and Milestones (POA&M) for each security risk. The ECM Authorizing Official signed the Cloud Security Assessment Report on February 10, 2021; therefore, ECM management officials had until April 10, 2021, (60 calendar days) to create the POA&Ms for the nine system security risks. In April 2021, ECM management officials opened nine POA&Ms with initial planned completion dates ranging from April 30, 2022, to May 2, 2022, in response to these risks. Figure 1 summarizes our analysis of the nine POA&Ms created for the risks identified in the initial security assessment.

[3] IRS, *Cloud Security Assessment Report, Information Technology Enterprise Case Management - Release 1, Version 1.3* (Feb. 3, 2021).

Figure 1: Summary of ECM System POA&M Results

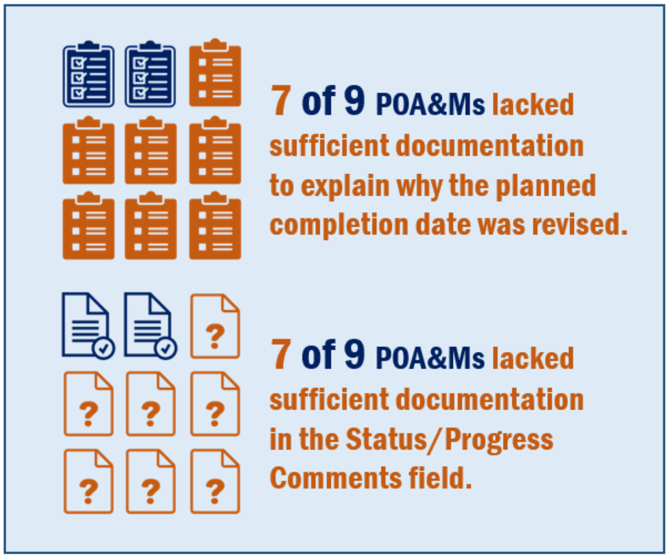


The IRS is required to create POA&Ms within 60 calendar days from when the weakness is identified for systems with a moderate security classification, such as the ECM system. Our review of the nine ECM system POA&Ms found that only three were created timely.

Source: Treasury Inspector General for Tax Administration's analysis of IRS POA&M documentation.

In June 2022, the Cybersecurity function re-evaluated approximately one-third of the cloud security controls for the ECM system. In June 2022, we again reviewed each of the nine POA&Ms and found that six (67 percent) were classified as late and the remaining three were classified as either completed, validated, or accepted. In addition, we determined that only two (22 percent) of the nine POA&Ms met agency documentation requirements. Figure 2 summarizes specific documentation issues we identified with the POA&Ms.

Figure 2: Specific POA&M Documentation Issues Identified As of June 6, 2022



7 of 9 POA&Ms lacked sufficient documentation to explain why the planned completion date was revised.

7 of 9 POA&Ms lacked sufficient documentation in the Status/Progress Comments field.

Source: Treasury Inspector General for Tax Administration's analysis of IRS POA&M documentation.

The IRM requires that a POA&M be developed for information systems to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the security controls assessment and to reduce or eliminate known vulnerabilities. In addition, it requires that the IRS create POA&Ms within 60 calendar days of identifying the weakness for systems with a moderate security classification. The IRM requires updating existing POA&Ms at least monthly based on the findings from the security control assessments, security impact analyses, and continuous monitoring activities. Lastly, an agency security policy requires comments explaining the new due date when revising a POA&M.[4]

Cybersecurity function management officials stated that the IRS followed the Enterprise Federal Information Security Modernization Act (FISMA) POA&M Standard Operating Procedure guidelines that require semiannual updates when the POA&M due date is more than 12 months away and quarterly updates when the POA&M due date is within 12 months. However, the FISMA POA&M Standard Operating Procedure is based on the standard Information Technology Security Policy IRM, not the IRM that governs cloud systems. The IRS Cloud Computing Security Policy IRM specifically states that the requirement to update POA&Ms monthly is defined by FedRAMP and supersedes the standard Information Technology Security Policy. Failure to timely update the POA&Ms increases the risk that appropriate resources are not directed to remediate system vulnerabilities in a timely manner.

Management Action: During our audit work, the IRS issued guidance stating that cloud systems must comply with the IRS Cloud Computing Security Policy IRM requiring POA&Ms be updated at least monthly. In addition, the IRS updated all six of the late POA&Ms as of June 6, 2022, which included comments explaining due date changes and progress updates. Three of these six POA&Ms are now designated as completed. One POA&M was cancelled and re-opened as an Enterprise Operations function program level POA&M with a completion date of October 31, 2023. One POA&M was partially completed with the remaining work scheduled for completion by February 2023. The final remaining POA&M is scheduled to be completed in March 2023.

Actions Were Taken to Address or Track Identified Security Risks

In June 2022, the Cybersecurity function performed an annual assessment of 42 ECM security controls governing the ECM cloud environment that resulted in the identification of five risks. We reviewed the five risks identified in the June 2022 Cloud Security Assessment Report and found that all five risks were previously reported in the February 2021 Cloud Security Assessment Report. We analyzed each of the five risks and found that:

- One had an existing POA&M in which the risk was subsequently accepted in June 2022.
- One had an existing POA&M that was remediated in August 2022.
- One had an existing open program-level POA&M.

As a result, these three risks did not require a new POA&M. The remaining two risks had previous POA&Ms that were closed. Because the two issues reoccurred, the IRS created two new POA&Ms, each with an April 24, 2023, due date.

[4] IRS, *Enterprise FISMA Plan of Action and Milestones Standard Operating Procedures* (June 18, 2020).

The ECM System Security Plan states that the on-premise production servers reside within the Enterprise Linux Platform. Between February and April 2022, the Cybersecurity function assessed security controls for the Linux environment. We reviewed the Enterprise Linux Platform's Security Assessment Report and found that in June 2022, the Cybersecurity function's Security Risk Management office issued four system security risks to the Enterprise Operations Authorizing Official responsible for the Linux environment. In June 2022, Enterprise Operations management officials opened four POA&Ms with initial planned completion dates in June 2023 in response to these risks. We analyzed each of the four POA&Ms and found that one was completed in October 2022. The remaining three POA&Ms are scheduled to be completed in June 2023.

Linux Servers Do Not Have Malicious Code Protection

In February 2021, the Cybersecurity function determined that both production servers that reside in the cloud for the ECM system lacked required malicious code protection. The National Institute of Standards and Technology requires malicious code protection at system entry and exit servers.[5]

In April 2021, ECM management officials created a POA&M to address this risk with the ECM system with a planned completion date of May 2022. In February 2022, we met with ECM management officials who stated that the lack of malicious code protection for the ECM servers was an enterprise-wide issue for Linux servers, and it was outside of their control to resolve. In July 2022, approximately 17 months after the weakness was found, the IRS opened a program-level POA&M assigned to the Enterprise Operations function and subsequently cancelled the POA&M assigned to the ECM system. According to IRS management officials, the IRS could reduce the length of time to identify and engage the appropriate resources if a process or team existed at the executive level to evaluate enterprise-wide risks to determine ownership, remediation, and implementation. We are currently conducting a separate review of the POA&M process.

The National Institute of Standards and Technology requires malicious code protection at system entry and exit servers within the organization.

In February 2021, the Cybersecurity function determined that both production servers that reside in the cloud for the ECM system lacked required malicious code protection. Although the IRS took steps to address the risk, the IRS lacks a consistent IRM policy for malicious code protection for Linux servers that can be used to evaluate both the cloud and on-premise servers.

In August 2022, we met with management officials from the Enterprise Program Management Office, Enterprise Operations, and Cybersecurity functions to discuss the lack of malicious code protection on ECM cloud servers and the new program-level POA&M. We determined that the program-level POA&M opened in July 2022 was incorrectly written specifically for the on-premise Linux servers that the IRS exempts from the malicious code protection requirements, as National Institute of Standards and Technology guidance does not provide an exemption for on-premise Linux servers. Because the ECM system uses servers governed by

[5] National Institute of Standards and Technology, Special Publication 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Feb. 2020).

both IRMs, the lack of consistency between the IRMs created confusion as to which policy applied to the ECM malicious code protection security finding. Specifically:

- The Information Technology Security Policy states that signature-based malicious code protection mechanisms shall be employed at system entry and exit points to detect and eradicate malicious code. An exception to the above requirement is Linux systems functioning as a server on the internal, trusted network and not functioning as system entry or exit points. These systems are not required to deploy anti-virus software; all other Linux systems are still required to deploy anti-virus software.
- The Cloud Computing Security Policy states that the Cloud Service Provider shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. This IRM does not include an exemption to this requirement.

During the meeting, we clarified that the Cloud Computing Security Policy IRM takes precedence and that the ECM servers in the cloud required malicious code protection. Failure to employ malicious code protection mechanisms could result in a compromise of the information system that a malicious code protection tool could otherwise detect for mitigation.

Management Action: During our audit work, the Enterprise Operations and Cybersecurity functions initiated a pilot test of an application to provide malicious code protection for Linux servers.

The Chief Information Officer should:

Recommendation 1: Ensure that the IRMs are consistent with National Institute of Standards and Technology guidelines for malicious code protection requirements for Linux servers.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will update the IRM to align with National Institute of Standards and Technology guidelines for malicious code protection requirements for Linux servers.

Recommendation 2: Complete the development and testing of an automated malicious code protection application and implement the application on all Linux servers.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will complete the development and testing of an automated malicious code protection solution and implement the solution on all applicable ECM on-premises Linux servers.
>
> > **Office of Audit Comment:** While we acknowledge the IRS's agreement, the planned corrective action does not fully address the recommendation. After the IRS completes the development and testing of an automated malicious code protection solution for Linux servers, it should implement the solution on all applicable Linux servers.

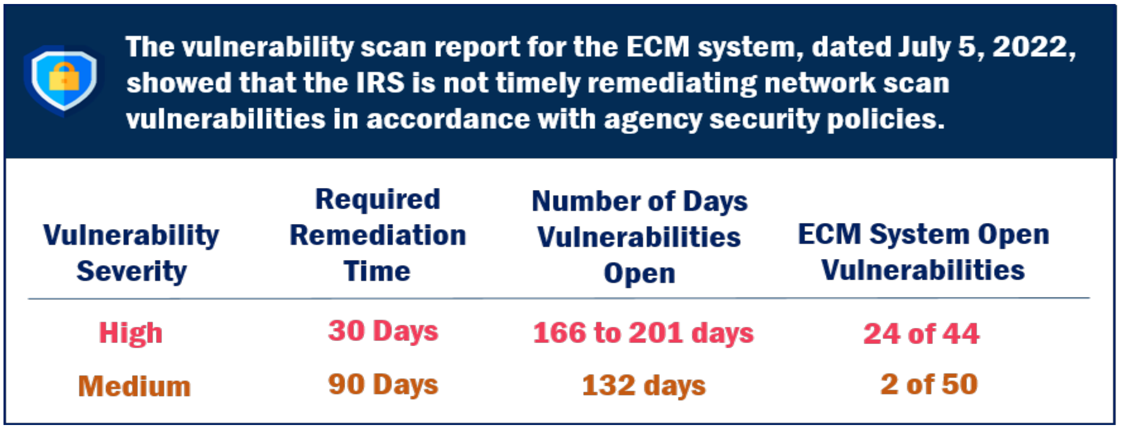
Recommendation 3: Ensure that all ECM servers in the cloud meet malicious code protection requirements.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will identify and implement malicious code protection on all ECM servers in the cloud to meet malicious code policy requirements.

Security Vulnerabilities Were Not Timely Remediated, but Actions Were Taken to Mitigate the Risks

We reviewed the July 2022 vulnerability scan report for the ECM system that identified 44 high- and 50 medium-risk vulnerabilities and found that the IRS did not timely remediate 24 high- and two medium-risk vulnerabilities in accordance with agency security policies. Figure 3 summarizes our analysis of the July 2022 vulnerability scan report.

Figure 3: ECM System Open Vulnerabilities



The vulnerability scan report for the ECM system, dated July 5, 2022, showed that the IRS is not timely remediating network scan vulnerabilities in accordance with agency security policies.

Vulnerability Severity	Required Remediation Time	Number of Days Vulnerabilities Open	ECM System Open Vulnerabilities
High	30 Days	166 to 201 days	24 of 44
Medium	90 Days	132 days	2 of 50

Source: Treasury Inspector General for Tax Administration's analysis of IRS vulnerability scan report.

The IRS accepted the risk for these vulnerabilities in November 2021 after remediating external facing applications and implementing other best practices to mitigate risks until software upgrades would remediate the issue for other vulnerable systems. A program-level POA&M was developed in March 2022 to track the remediation efforts of the 24 high- and two medium-risk vulnerabilities. The POA&M was designated as completed in December 2022.

The IRM requires that systems be scanned for vulnerabilities regularly using automated scanning tools. The IRS is also required to analyze vulnerability scan reports and security assessment reports, and remediate legitimate high-risk vulnerabilities within 30 calendar days and moderate-risk vulnerabilities within 90 calendar days. The IRS Enterprise FISMA POA&M Standard Operating Procedures require that POA&Ms be created within 30 calendar days (high-risk vulnerabilities) and 60 calendar days (medium- and low-risk vulnerabilities) of initial discovery of the vulnerability for vulnerabilities that cannot be fixed within the established time frames.

Production Servers Are Properly Configured

We reviewed a July 2022 configuration compliance report for the ECM system and found that each of the four production servers were compliant based on having average weighted compliance scores above 90 percent with no failed high-risk configuration compliance checks.

The IRM requires that the IRS identify, report, and correct system flaws; test for side effects; and install flaw remediation updates within 30 calendar days of an update's release. In addition, the IRM also requires:

- Incorporating flaw remediation in the organizational configuration management process.
- Automating monthly review of information system components for flaw remediation.
- Measuring the time between flaw identification and remediation.
- Establishing benchmarks for taking corrective actions.

User Account Management Controls Are Not Effective

User accounts were not deactivated or disabled timely

In our initial assessment of user account activity, we found that as of July 8, 2022, 401 (44 percent) of 917 user accounts had not signed into the ECM system for at least 90 calendar days. The IRS did not deactivate or disable 315 (79 percent) of the 401 user accounts, as required. However, the IRS deactivated 53 (13 percent) of the 401 accounts in accordance with agency security policies and quarantined an additional 33 (8 percent) of the 401 accounts within the ECM system.

The IRM requires that information systems shall automatically disable inactive user accounts after 90 calendar days. IRS personnel stated that the ECM system quarantined or deactivated inactive accounts within the application after 120 calendar days in accordance with the IRS Information Technology Security Policy IRM. However, the Cloud Computing Security Policy, which is more restrictive, requires accounts be deactivated after 90 calendar days of inactivity. We informed the Enterprise Program Management Office of this issue, and they created a POA&M to implement a change to the application in October 2022 that would apply the correct policy for disabling inactive user accounts. Not restricting user access in a timely manner would allow unauthorized access to taxpayer data and privacy information.

Management Action: During our audit work, we reviewed IRS documentation that illustrated how the ECM program modified the code to deactivate user accounts after 90 calendar days of inactivity.

Privileged user accounts were not monitored

We reviewed the last login information for ECM privileged user accounts in October 2022 and found four privileged user accounts were last logged into the ECM system in November or December 2021. The IRM requires the IRS to automatically disable inactive accounts after 90 days. IRS personnel stated that all of the privileged user accounts on the October 2022 report were active accounts. However, based on the last login dates, the IRS should have deactivated each of these four accounts due to inactivity.

In addition, the IRS was unable to provide evidence it reviewed ECM system access prior to our meeting about the issue. The IRM requires the IRS to monitor privileged role assignments and that IRS systems shall audit the execution of privileged functions. IRS personnel stated they were unable to obtain privileged user login information from their reporting tool and did not know exactly how long access to the login information had been unavailable. As a result, there was no evidence that the IRS monitored privileged account functions or activity.

According to the IRS, there is no communication between the ECM system and the system that authorizes privileged user access. Therefore, the IRS would need to deactivate access manually for inactive user accounts. By not monitoring the activity of accounts, the IRS is unaware of when inactive accounts reach a threshold that requires manual action, such as disabling an account or removing access privileges. Privileged user accounts are able to disable, circumvent, or alter implemented security safeguards. Failure to properly monitor and deactivate privileged user accounts increases the risk of unauthorized changes to the ECM system.

Recommendation 4: The Chief Information Officer should ensure that privileged user activity logs are regularly monitored and inactive accounts deactivated in accordance with agency security requirements.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will monitor ECM privileged user activity logs and regularly disable inactive privileged accounts in accordance with agency security requirements.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate whether the security controls over the ECM system were adequately protecting its data against unauthorized access. To accomplish our objective, we:

- Determined whether the ECM system complied with Federal and agency security requirements by reviewing and analyzing IRMs and agency authorization to operate procedures, including security assessment reports and POA&M documentation.
- Determined the effectiveness of the ECM system security controls implementation by reviewing and analyzing vulnerability scans, configuration compliance reports, and user account reports, and reviewing the IRS's efforts to remediate the identified malicious code protection weakness.

Performance of This Review

This review was performed with information obtained from the IRS's Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland, during the period February through December 2022. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Jason McKnight, Director; Kasey Koontz, Audit Manager; Mike Curtis, Acting Audit Manager; Mike Mohrman, Lead Auditor, Andrea Nowell, Senior Auditor, and Julia Woods, Information Technology Specialist (Data Analytics).

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: IRM guidance on *Information Technology Security, Policy and Guidance* and *Cloud Computing Security Policy*, and the IRS *Enterprise FISMA POA&M Standard Operating Procedures*. We evaluated these controls by interviewing Information Technology organization personnel; reviewing available documentation; and analyzing vulnerability scans, configuration compliance reports, user account reports, and IRS efforts to remediate vulnerabilities.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

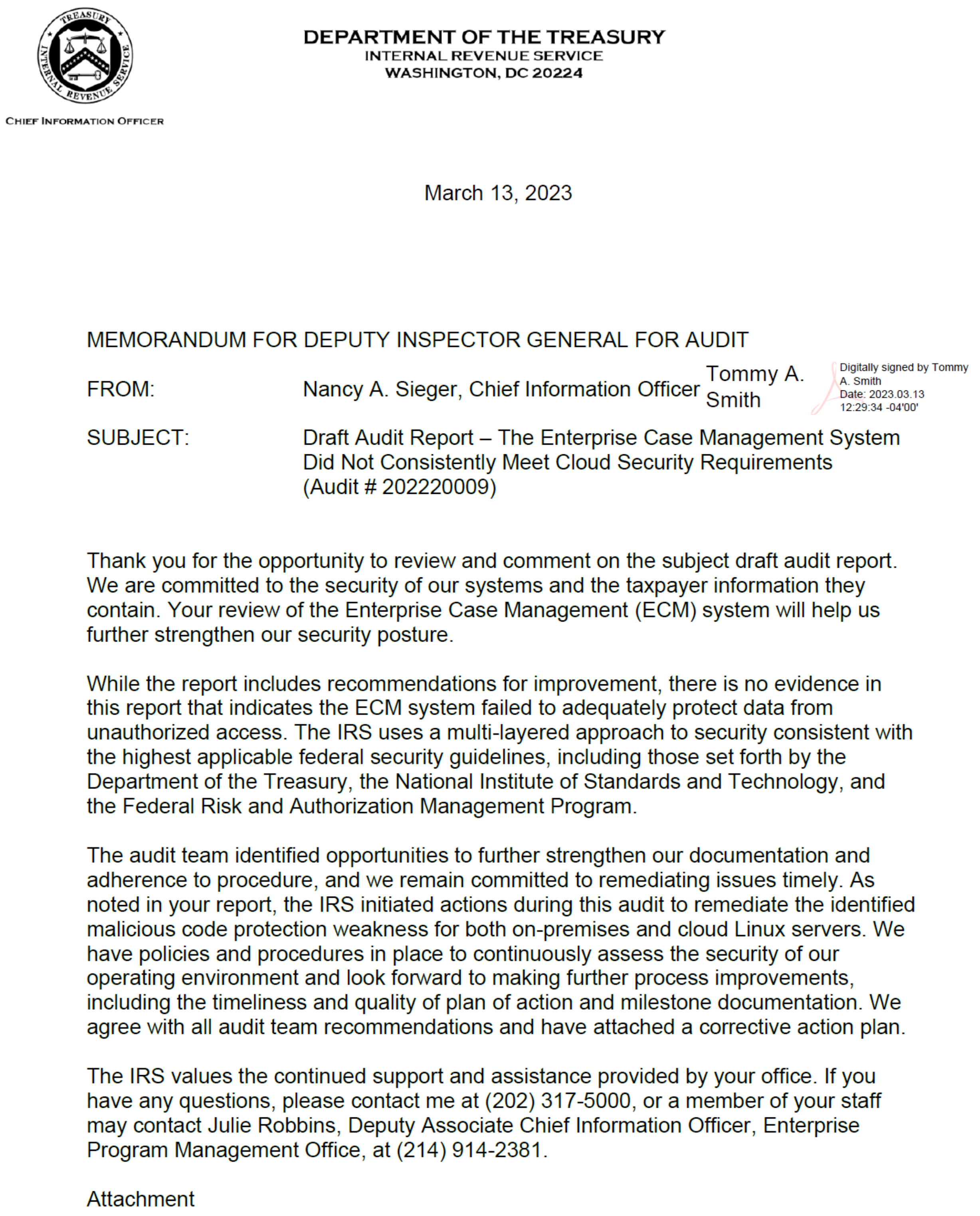
- Protection of Resources – Potential; two ECM production servers do not have malicious code protection (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We reviewed POA&M information and determined that the lack of malicious code weakness identified in the February 3, 2021, Cloud Security Assessment Report had not been remediated.

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

March 13, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger, Chief Information Officer Tommy A. Smith Digitally signed by Tommy A. Smith Date: 2023.03.13 12:29:34 -04'00'

SUBJECT: Draft Audit Report – The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements (Audit # 202220009)

Thank you for the opportunity to review and comment on the subject draft audit report. We are committed to the security of our systems and the taxpayer information they contain. Your review of the Enterprise Case Management (ECM) system will help us further strengthen our security posture.

While the report includes recommendations for improvement, there is no evidence in this report that indicates the ECM system failed to adequately protect data from unauthorized access. The IRS uses a multi-layered approach to security consistent with the highest applicable federal security guidelines, including those set forth by the Department of the Treasury, the National Institute of Standards and Technology, and the Federal Risk and Authorization Management Program.

The audit team identified opportunities to further strengthen our documentation and adherence to procedure, and we remain committed to remediating issues timely. As noted in your report, the IRS initiated actions during this audit to remediate the identified malicious code protection weakness for both on-premises and cloud Linux servers. We have policies and procedures in place to continuously assess the security of our operating environment and look forward to making further process improvements, including the timeliness and quality of plan of action and milestone documentation. We agree with all audit team recommendations and have attached a corrective action plan.

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 Julie Robbins, Deputy Associate Chief Information Officer, Enterprise Program Management Office, at (214) 914-2381.

Attachment

Audit# 202220009, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements*

RECOMMENDATION 1: The Chief Information Officer should ensure that Internal Revenue Manuals (IRMs) are consistent with National Institute of Standards and Technology guidelines for malicious code protection requirements for Linux servers.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will update IRM 10.8.1 to align with National Institute of Standards and Technology guidelines for malicious code protection requirements for Linux servers.

IMPLEMENTATION DATE: September 15, 2023

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should complete the development and testing of an automated malicious code protection application and implement the application on all Linux servers.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will complete the development and testing of an automated malicious code protection solution and implement the solution on all applicable Enterprise Case Management (ECM) on-premises Linux servers.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 3: The Chief Information Officer should ensure that all ECM servers in the cloud meet malicious code protection requirements.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will identify and implement malicious code protection on all ECM servers in the cloud to meet malicious code policy requirements.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

Audit# 202220009, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements*

RECOMMENDATION 4: The Chief Information Officer should ensure that privileged user activity logs are regularly monitored and inactive accounts deactivated in accordance with agency security requirements.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will monitor ECM privileged user activity logs and regularly disable inactive privileged accounts in accordance with agency security requirements.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Application	An information technology component of a system that uses information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
Authorization to Operate	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorizing Official	The person accountable for the security risks associated with information system operations and with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Cloud Service Provider	An entity offering cloud-based platform, infrastructure, application, or storage services.
Federal Risk and Authorization Management Program	A Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Internal Revenue Manual	The primary source of instructions to employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Plan of Action and Milestones	A document of the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities. The document is prepared for both systems and programs.
Privileged Accounts	Accounts with set “access rights” for certain users on a given system. Sometimes referred to as system or network administrative accounts.
Quarantined Accounts	Accounts that are disabled and whose user rights and permissions have been revoked.

Term	Definition
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
System Owner	Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and final disposition of an information system.
Vulnerability	A weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.

Appendix V

Abbreviations

ECM	Enterprise Case Management
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 23291
Washington, D.C. 20026

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