TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

[redacted] Platform Management Needs Improvement

September 28, 2021

Report Number: 2021-20-063

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

HIGHLIGHTS: [redacted] Platform Management Needs Improvement

Final Audit Report issued on September 28, 2021 **Report Number 2021-20-063**

Why TIGTA Did This Audit

This audit was initiated to determine the effectiveness of the [redacted] Platform systems security and operations.

The [redacted] Platform supports applications and systems used in tax administration and operations including the Affordable Care Act.

Impact on Taxpayers

Security weaknesses within the IRS's computer operations can allow an attacker the opportunity to access and control servers, which could begin to adversely affect the IRS's ability to meet its vision of upholding the integrity of the Nation's tax system and preserving the public trust. In addition, protecting critical assets and infrastructure helps reduce the risk of internal and external attacks on IRS assets that could potentially expose taxpayer data and information.

What TIGTA Found

The [redacted] Platform's inventory reconciliation process needs improvement. The official inventory did not reconcile with the Information System Contingency Plan, production server information was missing required data elements, and nine servers in the testing or development environment were misclassified as being in the production environment.

Administrative user accounts are limited to the least number of staff possible, and the IRS properly tracks modifications when administrative users execute commands. However, 79 (29 percent) of 272 [redacted] Platform user accounts reviewed did not access the [redacted] tool in 60 days or more and were not disabled or removed as required.

[redacted].

Finally, the configuration compliance-scanning tool reported that [redacted] production servers scanned in the [redacted] Platform were not in compliance with IRS configuration requirements, and [redacted].

What TIGTA Recommended

TIGTA made 11 recommendations including that the Chief Information Officer ensure that the official inventory repository is accurate and complete and implement an inventory reconciliation process; ensure that the Platform's servers are effectively defined; complete a review of group owners; retire older server versions and migrate to more current versions; ensure that the backlog of vulnerabilities is immediately resolved; review the Platform's patching processes; and ensure that vulnerabilities past remediation time frames are documented as required.

The IRS agreed with 10 recommendations and partially agreed with one recommendation. The IRS plans to implement an inventory reconciliation process; implement inventory verification controls to improve the accuracy and integrity of the data reported; ensure separated employees are not group owners and group owners are not also listed as users of the same group; retire older servers; and document vulnerabilities past remediation time frames as required. In addition, the IRS responded that it put a process in place to resolve the backlog of vulnerabilities and has reviewed the Platform's patching processes.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – [redacted] Platform Management Needs Improvement (Audit # 202120017)

This report presents the results of our review to determine the effectiveness of the [redacted] Platform systems security and operations. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] 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).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 1

The Platform Inventory Reconciliation Process Needs Improvement ..... Page 1

Recommendation 1: ..... Page 3

Recommendation 2: ..... Page 4

Some Access Controls Are in Place ..... Page 4

Users and Groups Are Not Effectively Managed ..... Page 4

Recommendations 3 and 4: ..... Page 6

Configuration Compliance Controls Are Insufficient ..... Page 6

Recommendations 5 through 7: ..... Page 8

Vulnerability Scanning and Remediation Are Insufficient ..... Page 9

Recommendation 8: ..... Page 11

Recommendations 9 through 11: ..... Page 12

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 13

Appendix II – Outcome Measures ..... Page 15

Appendix III – Management's Response to the Draft Report Page.16

Appendix IV – Glossary of Terms Page.23

Appendix V – Abbreviations Page.25

Background

The Internal Revenue Service (IRS) [redacted] Platform (hereafter called the Platform)[1] provides infrastructure supporting tax administration, including responsibilities associated with key provisions of the Affordable Care Act legislation.[2] Operating systems of the Platform include [redacted] and [redacted]. The Information Technology organization is responsible for deploying and maintaining the hardware and software configurations for the Platform.

We previously performed several audits that reviewed various elements of the Platform. In February 2016, we reported[3] that the IRS did not effectively manage the backup and restoration process for its Tier II environment. This environment includes, but is not exclusively limited to, [redacted] systems. In May 2018, we reported[4] that the IRS did not effectively mitigate critical and high-risk Integrated Data Retrieval System vulnerabilities. These vulnerabilities also included, but were not limited to, [redacted] systems in the Tier II environment. In December 2018,[5] we reported that a [redacted] migration project operated without appropriate governance leading to project delays. Finally, in June 2019,[6] we reported that software running on Tier I mainframes were not listed in the approved Enterprise Standards Profile Product Catalog or listed as archived or retired. These mainframes included, but were not exclusively limited to, the Platform.

Results of Review

The Platform Inventory Reconciliation Process Needs Improvement

The Internal Revenue Manual (IRM)[7] states that the IRS shall develop and maintain a comprehensive inventory of information systems and relevant security information for those systems. In addition, the Hardware User Guide[8] documents the minimum information that must be kept accurate and current in the official inventory. This includes but is not limited to *Assignment*, *Barcode*, *Serial Number*, and *Computer Name*.

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

[2] Patient Protection and Affordable Care Act (Affordable Care Act), Pub. L. No. 111-148, 124 Stat. 119 (2010).

[3] Treasury Inspector General for Tax Administration, Report No. 2016-20-019, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* (Feb. 2016).

[4] Treasury Inspector General for Tax Administration, Report No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).

[5] Treasury Inspector General for Tax Administration, Report No. 2019-20-008, [redacted] *Migration Project Was Delayed and Needs Improved Governance* (Dec. 2018).

[6] Treasury Inspector General for Tax Administration, Report No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019).

[7] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019).

[8] IRS, *Asset Management User and Network Services Hardware User Guide* (Nov. 14, 2017).

The User and Network Services function is responsible for managing the information technology hardware assets. The IRS uses the Hewlett Packard Asset Manager module[9] to track its hardware asset inventory. The IRS confirmed that Asset Manager is the official inventory for tracking the Platform's assets.

Inventory reconciliation

The IRM states that the IRS should develop and document an inventory of information system components that accurately reflects the current information system. We reviewed the inventories from the Information System Contingency Plan (ISCP), the vulnerability scanning tool, and the configuration scanning tool to reconcile with the official inventory. We also reviewed the most recent annual security control assessment performed from March 2020 through April 2020 and found that the IRS failed to reconcile the official inventory to the ISCP inventory. To assess the accuracy and completeness of the Platform inventory, we reconciled the January and February 2021 official inventory reports to the ISCP reports and identified variances between the inventories. Figure 1 provides the results of our review.

Figure 1: [redacted]

[redacted]

Source: Treasury Inspector General for Tax Administration analysis of data from the ISCP and official inventories.

In addition, we reviewed the February 2021 official inventory and found production servers with missing inventory data elements:

- *Asset Location* field was blank for 286 servers.
- *Serial Number* field was blank for seven physical servers.
- *Building Code* field was blank for two servers.

[9] The Hewlett Packard Asset Manager is a component of the Knowledge, Incident/Problem Service Asset Management system, which is the IRS's official asset inventory system.

The IRS stated that variance between the ISCP and the official inventory, as well as gaps in the completeness of the reports, is the result of the time required to collect, organize, and complete the review process of the ISCP and the official inventory's data. An inaccurate inventory can hinder the agency's ability to manage systems. Inaccurate inventory data also negatively affects systems that rely on the information within the official inventory, such as configuration and vulnerability scanning tool inventories.

We also found that nine servers in the official inventory are classified as being in the production environment; however, according to the configuration scanning tool these servers are in the testing or development environments. The IRS stated that the Server Signature File is used to set the *Environment*, the *General Support System*, and the *Project* fields in the official inventory. The Server Signature File is a file that resides locally on each server. The IRS stated that this discrepancy is due to an incorrect Server Signature File or the original file data were not populated correctly. Server misclassification can lead to vulnerabilities being excluded from prioritization and remediation efforts.

Scanning servers for vulnerabilities

The IRM states information systems and hosted applications shall be scanned for vulnerabilities every 30 days, prior to placing a new information system on an IRS network, and when new vulnerabilities potentially affecting the system or applications are identified and reported. The Enterprise Vulnerability Scanning process includes probes of communication services, operating systems, and applications to identify high-risk system weaknesses that could be exploited to gain unauthorized access to IRS networks and data. We compared the official inventory report dated February 18, 2021, to vulnerability scanning reports and found that [redacted]. This occurred because the IRS has not developed a process to effectively track all information technology assets leading to disparate asset counts in various systems' inventories. Without complete scanning of all production servers, the IRS cannot adequately define its current security posture because some critical vulnerabilities may go undetected.

Management Action: In response to this finding, the IRS started scanning 36 of the 41 servers as of July 2021. Three of the unscanned servers are retired and the remaining two are under investigation.

The Chief Information Officer should:

Recommendation 1: Ensure that the official inventory repository is accurate and complete and implement an inventory reconciliation process to ensure that administrative tools, such as vulnerability, configuration scanning tools, and the ISCP inventory align with the official inventory repository.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that the official inventory repository is accurate and complete and implement an inventory reconciliation process to ensure that administrative tools, such as vulnerability and configuration scanning tools, and the ISCP inventory align with the official inventory repository.

Recommendation 2: Ensure the Platform's servers are effectively defined to improve the accuracy and completeness of the data reported to the official inventory repository.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that the official inventory is accurate and complete and implement inventory verification controls to improve the accuracy and integrity of the data that define the server environment data reported to the official inventory repository.

Some Access Controls Are in Place

Control of users and groups is a core element of [redacted] system administration. Users and groups have a combination of permissions for files owned by a specific group. In the [redacted] operating system, the root account is a user account for administrative purposes, and typically has the highest access rights. The IRM states that in the [redacted] operating system, the root account shall be implemented and used by the least number of staff possible without degrading system availability. We judgmentally sampled[10] 30 servers and reviewed all user account information on each server. We verified that each of the 30 sampled servers had only one account with root level access.

The System Security Plan for the Platform states that the Cybersecurity function retrieves the system logs that would record the actions of anyone logged into a root account at the console. We reviewed over 1 million access log entries generated in January and February 2021 and found that the IRS properly tracks modifications when users execute commands as a root user.

Users and Groups Are Not Effectively Managed

The IRM states that the number of personnel with access to the platform shall be approved by a designated representative. The System Security Plan states that access to the Platform is granted through the [redacted] system process.[11] The system shall employ the concept of least privilege by limiting users' access to that necessary to accomplish assigned tasks and establish roles for the specific actions conducted within the operational environment. In addition, the IRM states that duties and responsibilities of functions shall be separated among different individuals so that no single individual shall have all necessary authority and system access to disrupt or corrupt a security process.

The [redacted] system recertification process for group owners and users needs improvement

The IRM states that a list of users shall be reviewed at a minimum every six months or when a change occurs. We reviewed [redacted] system reports of all the Platform's groups and found 21 unique groups, managed by 13 owners. According to the [redacted] Manager's Guide,[12] the owner of the group is responsible for establishing, updating, or removing a user from a

[10] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[11] The IRS is in the process of migrating from the [redacted].
[12] IRS, [redacted] *Manager's Guide*, (June 2017).

group, reassigning a user to a different manager within the [redacted] system, and recertifying a user. However, we found that the Platform has one user that is both a member and an owner of a group. [redacted].

We selected a judgmental sample of 21 users, one user from every group, to assess access recertification. We received user recertification reports for all 21 users as of March 2021. [redacted].

IRS personnel stated that the [redacted] system lacks the automated capability to complete an effective review for separated users, *i.e.*, employees, and to prevent an owner being a member of the same group. Without an effective review of the owners responsible for administering the group roles, accounts can be improperly managed and may violate separation of duty policies.

Inactive users within the **********2********** tool retain privileges

IRS procedures[13] state that the [redacted] is the chosen tool for managing elevated access to the Platform in order to meet guidelines from Homeland Security Presidential Directive 12.[14] The IRM states that privileged accounts on an information system shall be restricted to designated system administrators. In addition, the IRM states that accounts that are inactive for a period of 60 days shall be disabled and accounts that are inactive for a period of 365 days shall be removed.

The [redacted] tool is a commercial-off-the-shelf product that the IRS uses as an enterprise-wide solution for password management. We completed a detailed assessment of 272 users with access to the Platform via the [redacted] tool. The [redacted] tool history report from February 2021 indicated that [redacted].

- [redacted].
- [redacted].
- [redacted].

We determined that the IRS lacks a process to review access to the [redacted] tool. As a result, these [redacted].

[13] IRS, *Privileged Access Management Standard Operating Procedures* (Sept. 2020).

[14] Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2004).

The Chief Information Officer should:

Recommendation 3: Complete a review of group owners to ensure that separated employees are not group owners and group owners are not also listed as users of the same group.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that separated employees are not group owners and group owners are not also listed as users of the same group.

Recommendation 4: Create an automated process to ensure that all user accounts have logged on within the allotted time frames and disable or remove inactive users.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will create an automated process to ensure that all user accounts have logged on within the allotted time frames and disable or remove inactive users.

Configuration Compliance Controls Are Insufficient

The IRM specifies secure configurations for all operational information technology and communication systems. Further, the IRM requires the employment of automated capabilities to maintain an up-to-date, complete, accurate, and readily available baseline configuration of information systems. The IRS uses a configuration scanning tool to scan for configuration compliance and the resulting output is transmitted to a dashboard for review.

Production servers are not in compliance with configuration requirements

According to the Department of Homeland Security,[15] each vulnerability found on a network should be given a numeric score, meant to represent the risk of not mitigating that vulnerability. Per the IRS user guide,[16] hosts (*e.g.,* servers) are considered compliant if their weighted compliance score is [redacted].

We met with a Director, Security Operations, and other Enterprise Operations function officials and they provided documentation that stated between April 2020 and April 2021, they remediated approximately 19,000 [redacted] vulnerabilities. However, our review of the configuration scanning tool dashboard output found that [redacted].

Enterprise Operations management stated that an [redacted]. During the audit, the IRS provided a plan to replace 1,025 [redacted] servers and 781 [redacted]

[15] Department of Homeland Security, *Continuous Diagnostics and Mitigation, Agency-Wide Adaptive Risk Enumeration Technical Design* (Nov. 1, 2017).

[16] IRS, *Hindustan Computer Limited BigFix Customer Success Manager Dashboard User Guide, Ver. 1.0* (Nov. 19, 2020).

servers by December 2023. Configuration vulnerabilities that lack remediation can allow an attacker the opportunity to access and control servers.

Configuration vulnerability age is not tracked

The IRM[17] provides time frames to remediate vulnerabilities detected on servers. In January 2020, the IRS issued an interim memorandum with updated remediation timelines. We found the configuration scanning tool report provides limited historical information, such as client last seen dates. Our review of the scan report found the IRS does not keep track of when a vulnerability was first seen or remediated.

According to the IRS, the client last seen date shows when the configuration scanning tool last scanned the server. The IRS further stated the configuration scanning tool [redacted].

Checklists used in the configuration compliance-scanning tool are outdated and differences in requirements are not documented

According to the National Institute of Standards and Technology,[18] common secure configuration, including configuration checklists, provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products. Per the IRM,[19] IRS Security Requirements Checklists for Operating System platforms are derived from Defense Information Systems Agency (DISA) security guides. Cybersecurity function management stated it is the IRS's responsibility to perform adjudication reviews and test vendor-provided checklists to ensure that vendor-provided checks align with IRS Security Requirements Checklists.

To determine whether the adjudication review was completed, we obtained documentation for the adjudication reviews completed by the IRS for the [redacted] Operating Systems in production. We found that the vendor-provided checklists in use by the configuration-scanning tool had undergone adjudication reviews in [redacted]. However, the adjudicated vendor-provided checklists used in the configuration scanning tool were not the most current DISA security guide. The vendor-provided [redacted] checklist used an outdated DISA security guide released [redacted]. We could not find a DISA revision history for the vendor-provided [redacted] checklist; however, the IRS stated it is aware of needed improvements.

[17] IRM 10.8.50, *Information Technology Security, Service-wide Security Patch Management* (Nov. 25, 2020).

[18] National Institute of Standards and Technology, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

[19] IRM 10.8.15, *Information Technology Security, General Platform Operating System Security Policy* (Dec. 2020).

We found that the Cybersecurity function issued a policy, dated July 2020, stating the current configuration security guidance imposed gaps that negatively affect stakeholders. One of the gaps mentioned is out-of-date checklists. According to the policy, the IRS is mitigating these gaps by revising its processes to update baselines to ensure that the most up-to-date baseline security guidance is available. This occurred because the vendor-provided checklist review and approval process prolongs the implementation of DISA Security and Implementation Guide releases. In addition, the IRS relies on a vendor to implement the Security Requirements Checklists in the configuration-scanning tool, which extends the implementation period. When outdated Security Requirements Checklists are used in the configuration-scanning tool, critical vulnerabilities that hackers can exploit may not be timely detected.

The National Institute of Standards and Technology requires organizations to identify, document, and approve any deviations from established configuration settings based on defined operational requirements. We reviewed the IRS's adjudication of the vendor-provided checklists used in the configuration-scanning tool and found that the IRS reviews the vendor-provided checklists and documents deviations from IRM requirements. However, the review does not document when a check required by the IRS's Security Requirements Checklists are not included in the vendor-provided checklists.

The IRS lacks an adjudication process that would ensure that all security requirements are accounted for in the vendor-provided checklists used in the configuration compliance-scanning tool. An official stated that the IRS is in the process of updating the vendor checklist adjudication process to account for security requirements that are not included in the vendor-provided checklists. Without ensuring that this process occurs, critical and unique security requirements may not be applied to IRS systems.

The Chief Information Officer should:

Recommendation 5: Retire older [redacted] and migrate to more current [redacted] in accordance with the documented migration plan.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Applications Development, will lead the efforts to retire [redacted] and migrate to more current [redacted] in accordance with the documented [redacted] Lifecycle Program migration plan, contingent on budget approval.

Recommendation 6: Evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance-scanning tool.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance-scanning tool.

Recommendation 7: Update the checklist adjudication process to include a reconciliation, documentation, and tracking of checks required by the IRS but not included in the vendor checklist used by the configuration compliance-scanning tool. Also, ensure that Security Requirements Checklists are timely updated with the current DISA security guide and implemented.

Management's Response: The IRS partially agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will update the checklist adjudication process to include a reconciliation, documentation, and tracking of checks required by the IRS but not included in the vendor checklist used by the configuration compliance-scanning tool. Also, the IRS will ensure that Security Requirements Checklists are timely updated with the current DISA security guide and implemented to the extent practicable dependent on automated check content availability from the Continuous Diagnostic and Mitigation sensor tool vendor.

Office of Audit Comment: The IRS's corrective action addresses the intent of our recommendation. However, if the IRS depends on the Continuous Diagnostic and Mitigation sensor tool vendor to provide automated checks, this could result in the IRS being two or three versions behind DISA security guides. The IRS should document this gap in a Risk-Based Decision or update the current Service Level Agreement with the vendor to provide automated checks for the most current security guides in a reasonable time frame.

Vulnerability Scanning and Remediation Are Insufficient

Credentialed scans are not performed on all production servers

According to the IRM, the IRS shall implement privileged access authorization to all information system components for selected vulnerability scanning activities to facilitate more thorough scanning. The Enterprise Vulnerability Standards[20] state that agent-based scanning eliminates the need for service accounts previously used in remote credential scans. We reviewed two vulnerability scan reports from February 2021 and found [redacted]. The vulnerability scanning tool was implemented less than a year ago and, as a result, the IRS is still defining processes to identify and remediate servers that are not receiving appropriate scans. [redacted].

Management Action: In response to this finding, the IRS has provided evidence that they are currently performing credentialed scans on [redacted].

Vulnerabilities are not timely remediated

Interim IRM guidance applies a vulnerability metric to assign a severity rating and remediation time frames as shown in Figure 3.

[20] IRS, *Enterprise Vulnerability Scanning Standard Operating Procedures* (Aug. 2020).

Figure 3: Vulnerability Severity Rating Scale and Remediation Time Frames

Vulnerability Severity Level	Expected Remediation Time Frame
Critical	Internet Accessible systems identified in Cyber Hygiene Reports - 15 days All other systems 30 days
High	Internet Accessible systems identified in Cyber Hygiene Reports - 30 days High Value Assets - 60 days All other systems 90 days
Medium	120 days
Low	180 days

Source: IRM 10.8.50.

Figure 4 shows a summary of vulnerabilities in the Platform and their associated severity level rating that are past the remediation time frames as of February 23, 2021.

Figure 4: [redacted]

[redacted]

Source: Treasury Inspector General for Tax Administration analysis of Platform vulnerabilities as of February 23, 2021.

[redacted]

- [redacted].
- [redacted].
- [redacted].
- [redacted].

Due to the lack of appropriate management oversight, the IRS is not remediating vulnerabilities in accordance with IRM requirements. Failure to resolve existing system security weaknesses compromises the security posture of the Platform.

In addition, we found one instance where [redacted]. Unpatched vulnerabilities allow bad actors to conduct attacks against the Platform infrastructure. Unpatched vulnerabilities may also provide entry points into a network.

Vulnerabilities open past remediation time frames are not effectively documented and tracked

The IRM states that in the event remediation of a vulnerability is delayed due to agency needs, the information system owner shall document the justification in a Plan of Action and Milestones. Other IRS policies and procedures stipulate that a Plan of Action and Milestones or a Risk-Based Decision should be used to document and track vulnerabilities that are not remediated within the required time frame. We judgmentally sampled 12 servers with [redacted]. We found that the IRS did not have a documented Plan of Action and Milestones or Risk-Based Decision to track the remediation of any of the [redacted] we sampled. Due to the lack of management oversight, the IRS is not ensuring that unremediated vulnerabilities are being tracked as required. Without tracking vulnerabilities, there is a possibility some vulnerabilities will not be remediated.

The Chief Information Officer should:

Recommendation 8: Ensure that credentialed scans are completed on the Platform's servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure that credentialed scans are completed on the Linus Platform's servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

Recommendation 9: Ensure that the backlog of vulnerabilities in the Platform is immediately resolved.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, has put a process in place to track and immediately resolve the backlog of vulnerabilities in the Platform.

Recommendation 10: Review the Platform's patching processes to ensure that a process exists to track all patch-related vulnerabilities.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, has reviewed the Platform's patching processes to ensure that a process exists to track all patch-related vulnerabilities.

Recommendation 11: Ensure that vulnerabilities past remediation time frames are documented with Risk-Based Decisions or Plans of Action and Milestones as required.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, will ensure that remaining vulnerabilities past remediation time frames are documented with Risk-Based Decisions or Plans of Action and Milestones as required.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine the effectiveness of the Platform's system security and operations. To accomplish our objective, we:

- Reviewed relevant IRMs and evaluated access control reports to determine the restrictions for privileged users. We interviewed IRS employees to determine the access-related controls in place for root users of the Platform. We selected a judgmental sample[1] of 30 servers stratified to account for operating system version and asset type from the population of 1,224 servers to determine root level user access restriction. We also selected a judgmental sample of 21 users, one user from every user group, from a population of 272 users to assess access recertification.
- Reviewed server security configuration policy compliance reports to identify high vulnerabilities, and interviewed IRS employees regarding security policies and procedures to determine whether configuration vulnerabilities were timely remediated within agency security policies.
- Reviewed and analyzed multiple security vulnerability reports to identify critical and high-risk vulnerabilities. We also interviewed IRS employees to review and validate our analysis to determine whether security vulnerabilities were timely remediated according to guidance established by the IRM. In addition, we selected a judgmental sample of 12 of 261 servers with 10 or more non-remediated critical vulnerabilities to determine if vulnerabilities not timely remediated are tracked as required. We also selected a judgmental sample of 36 of 228 servers with four or more non-remediated high vulnerabilities to determine if vulnerabilities not timely remediated are tracked as required.
- Reviewed relevant IRMs and inventory reports to determine the completeness and accuracy of the Platform server inventory. We also reviewed the annual inventory certification process to determine whether inventory discrepancies were identified.

Performance of This Review

This review was performed with information obtained from the Office of the Chief Information Officer located in the New Carrollton Federal Building in Lanham, Maryland, during the period October 2020 through June 2021. 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, Audit

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Manager; Nicholas Reyes, Lead Auditor; Daniel Preko, Senior Auditor; and Lance Welling, 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 policies related to the logical control of information technology, Standard Operating Procedures for user access, baseline system configurations, vulnerability scanning, and inventory of the Platform production systems. We evaluated these controls by interviewing Cybersecurity, Enterprise Operations, and User and Network Services function personnel. We also reviewed documentation including policies and procedures related to user access, configuration scanning, vulnerability scanning, and inventory management, and reports of scanning results.

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:

- Protection of Resources – Potential; 41 of 1,224 servers were not scanned by the vulnerability scanning tool (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We compared the IRS inventory report dated February 18, 2021, to vulnerability scanning reports generated on February 23, 2021. Our analysis determined that there were 41 servers that have not been scanned by the vulnerability scanning tool within the Platform boundary.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 705 unique servers had 2,558 vulnerabilities that exceeded the IRS policy for timely remediation (see Recommendation 10).

Methodology Used to Measure the Reported Benefit:

We compared the IRS inventory report dated February 18, 2021, to vulnerability scanning reports generated on February 23, 2021. An analysis by our data analytics team determined the 2,558 vulnerabilities occurred on 705 unique servers within the Platform boundary. We also analyzed the vulnerability severity level and the age of the 2,558 vulnerabilities to determine the timeliness of remediation actions.

Appendix III

Management's Response to the Draft Report

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

CHIEF INFORMATION OFFICER

September 1, 2021

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger /s/ Nancy A. Sieger
Chief Information Officer

SUBJECT: Response to Draft Audit Report – [redacted] Platform Management Needs Improvement (e-trak # 2021-39804).

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate the time you have taken to assess the effectiveness of the [redacted] Platform systems' security and operations which supports applications and systems used in tax administration. IRS agrees that protecting critical assets and infrastructure helps reduce the risk of internal and external attacks on IRS assets that could potentially expose taxpayer data and information.

Prior to this review, the IRS has taken positive steps to improve asset security through the implementation of the Continuous Diagnostics and Mitigation (CDM) Phase I and [redacted] vulnerability scanning. These tools have allowed more rapid access to vulnerability data and brought the IRS in compliance with current industry standards for security assessment. Since the implementation of CDM Phase I the IRS remediated approximately 19,000 [redacted] vulnerabilities. Your assessment has helped us identify areas in which we can continue to improve the utilization of these new capabilities.

We concur with the two recommended outcome measures. In response to your recommendations, we have attached our corrective action plan and are committed to implementing them.

The IRS values the continued support and assistance provided by your office. Should you have any questions, please contact me or a member of your staff may contact Frank Henderson, Director, Enterprise Operations, Security Operations and Standards Division at 618-260-3680.

Attachment

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

RECOMMENDATION 1
The Chief Information Officer should ensure that the official inventory repository is accurate and complete and implement an inventory reconciliation process to ensure that administrative tools, such as vulnerability and configuration scanning tools, and the ISCP inventory align with the official inventory repository

CORRECTIVE ACTION 1
The IRS agrees with this recommendation. The Associate Chief Information Officer, EOps will ensure that the official inventory repository is accurate and complete and implement an inventory reconciliation process to ensure that administrative tools, such as vulnerability and configuration scanning tools, and the ISCP inventory align with the official inventory repository.

IMPLEMENTATION DATE
December 15, 2023

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION Monitoring Plan
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2
The Chief Information Officer should ensure the Platform's servers are effectively defined to improve the accuracy and completeness of the data reported to the official inventory repository.

CORRECTIVE ACTION 2
The IRS agrees with this recommendation. The Associate Chief Information Officer, EOps will ensure the official inventory is accurate and complete and implement inventory verification controls to improve the accuracy and integrity of the data that defines the server environment data reported to the official inventory repository.

IMPLEMENTATION DATE
October 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION Monitoring Plan
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

RECOMMENDATION 3
The Chief Information Officer should complete a review of group owners to ensure that separated employees are not group owners and group owners are not also listed as users of the same group.

CORRECTIVE ACTION 3
The IRS agrees with this recommendation. The Associate Chief Information Officer, EOps will ensure that separated employees are not group owners and group owners are not also listed as users of the same group.

IMPLEMENTATION DATE
March 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4
The Chief Information Officer should create an automated process to ensure that all user accounts have logged on within the allotted time frames and disable or remove inactive users.

CORRECTIVE ACTION 4
The IRS agrees with this recommendation. The Associate Chief Information Officer, EOps will create an automated process to ensure that all user accounts have logged on within the allotted time frames and disable or remove inactive users.

IMPLEMENTATION DATE
July 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

RECOMMENDATION 5
The Chief Information Officer should retire older [redacted] and migrate to more current [redacted] in accordance with the documented migration plan.

CORRECTIVE ACTION 5
The IRS agrees with this recommendation. The Associate Chief Information Officer, AD will lead the efforts to retire [redacted] and migrate to more current [redacted] in accordance with the documented LLP migration plan, contingent on budget approval.

IMPLEMENTATION DATE
December 15, 2023

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 6
The Chief Information Officer will evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance scanning tool.

CORRECTIVE ACTION 6
The IRS agrees with this recommendation. The Associate Chief Information Officer, Cybersecurity will evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance scanning tool.

IMPLEMENTATION DATE
October 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

RECOMMENDATION 7
The Chief Information Officer should update the checklist adjudication process to include a reconciliation, documentation, and tracking of checks required by the IRS but not included in the vendor checklist used by the configuration compliance-scanning tool. Also, ensure that Security Requirements Checklists are timely updated with the current DISA security guide and implemented.

CORRECTIVE ACTION 7
The IRS partially agrees with this recommendation. The Associate Chief Information Officer, Cybersecurity will update the checklist adjudication process to include a reconciliation, documentation, and tracking of checks required by the IRS but not included in the vendor checklist used by the configuration compliance-scanning tool. Also, IRS will ensure that Security Requirements Checklists are timely updated with the current DISA security guide and implemented to the extent practicable dependent on automated check content availability from the CDM sensor tool vendor.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 8
The Chief Information Officer should ensure that credentialed scans are completed on the Platform's servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

CORRECTIVE ACTION 8
The IRS agrees with this recommendation. The Associate Chief Information Officer, Cybersecurity will ensure that credentialed scans are completed on the [redacted] Platform's servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 9
The Associate Chief Information Officer should ensure that the backlog of vulnerabilities in the Platform is immediately resolved.

CORRECTIVE ACTION 9
The IRS agrees with this recommendation. The Associate Chief Information Officer EOps has put a process in place to track and immediately resolve the backlog of vulnerabilities in the [redacted] Platform.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 10
The Chief Information Officer should review the Platform's patching processes to ensure that a process exists to track all patch-related vulnerabilities.

CORRECTIVE ACTION 10
The IRS agrees with this recommendation. The Associate Chief Information Officer, EOps has reviewed the Platform's patching processes to ensure that a process exists to track all patch-related vulnerabilities.

IMPLEMENTATION DATE
Implemented May 15, 2021

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

Attachment

Draft Audit Report – Review of the [redacted] Platform (Audit #202120017)

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 11
The Chief Information Officer should ensure that vulnerabilities past remediation time frames are documented with Risk Based Decisions or Plans of Action and Milestones as required.

CORRECTIVE ACTION 11
The IRS agrees with this recommendation. The Associate Chief Information Officer EOps will ensure that remaining vulnerabilities past remediation time frames are documented with Risk Based Decisions or Plans of Action and Milestones as required.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL(S)
Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

Appendix IV

Glossary of Terms

Term	Definition
Access Controls	Policies uniformly enforced across all subjects, *i.e.*, users, 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: passing the information to unauthorized subjects or objects; granting its privileges to other subjects; changing one or more security attributes on subjects, objects, the information system, or system components; choosing the security attributes to be associated with newly created or modified objects; or 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 above constraints.
Application	A software program hosted by an information system.
Credential	An object or data structure that authoritatively binds an identity to at least one authenticator possessed and controlled by a subscriber.
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, relating to progress and performance.
Hardening	Providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as 'defense in depth.' Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level, and all the sublevels in between. A hardened computer system is a more secure computer system.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers.
Internal Revenue Manual	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.
Middleware	Software that functions at an intermediate layer between applications and operating system or database management system or between client and server.
[redacted] System	A web-based application 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 application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.

Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
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 Congress.
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
Privileged Accounts	Accounts with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.
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.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost-effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or National Institute of Standards and Technology guidelines, whether related to a technical, operational, or management control.
Security Technical Implementation Guide	Based on Department of Defense policy and security controls, implementation guides are geared to a specific product and version. They contain all requirements that have been flagged as applicable for the product.
Security Vulnerabilities	Weakness in configuration or design that attackers may target and exploit.
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.
User	Individual, or (system) process acting on behalf of an individual, authorized to access an information system.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.

Appendix V

Abbreviations

DISA	Defense Information System Agency
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISCP	Information System Contingency Plan
[redacted]	[redacted]
[redacted]	[redacted]

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 589

Ben Franklin Station

Washington, D.C. 20044-0589

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