TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform

September 15, 2025

Report Number: 2025-200-035

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

HIGHLIGHTS: The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform

Final Audit Report issued on September 15, 2025 **Report Number 2025-200-035**

Why TIGTA Did This Audit

This audit was initiated to determine the effectiveness of the [redacted] Platform (hereafter referred to as the platform) systems security and whether the IRS effectively implemented prior recommendations.

The minimum system security requirements of the platform include monitoring for and remediation of vulnerabilities, ensuring configuration compliance, conducting a system inventory, and protecting against malicious code.

We previously reviewed various elements of the platform. In September 2021, we reported several deficiencies including insufficient vulnerability scanning and remediation and the need for improvements in the platform inventory reconciliation process.

Impact on Tax Administration

The platform supports applications and systems used in tax administration and operations including the Affordable Care Act. The IRS relies on the platform to accomplish its mission of providing services to other federal agencies and the public.

Without effective security controls, the IRS's systems are vulnerable to actions taken by individuals with malicious intent which could lead to the potential exposure of sensitive taxpayer data and/or result in damaging the reputation of the IRS.

What TIGTA Found

The IRS's security vulnerability controls have improved; however, vulnerabilities remain. We confirmed that the IRS implemented several of our previous recommendations. For example, the IRS completed credentialed scans on the platform servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications. In addition, the IRS implemented a historical age tracking capability to include the last pass and last fail dates; and implemented [redacted] protection for platform servers.

Security vulnerabilities continue to exceed remediation time frames. We found [redacted] vulnerabilities across [redacted] unique servers that exceeded the IRS policy for timely remediation. The IRS followed established policy and either developed a Plan of Action and Milestones (*i.e.*, a corrective action plan) or a Risk Based Decision (*i.e.*, a documented acceptance of risk) for these existing vulnerabilities.

However, we found unresolved configuration compliance vulnerabilities in the IRS production servers that did not have a Plan of Action and Milestones or a Risk Based Decision. Specifically, we identified [redacted] unique servers with [redacted] medium and [redacted] low configuration compliance vulnerabilities that exceeded the IRS policy for timely remediation. The [redacted] all reside on servers with configuration vulnerabilities. These systems are responsible for receiving and processing [redacted] identifying [redacted] compliance, and [redacted]

Further, [redacted] production servers did not have [redacted] protection installed or documented Plans of Action and Milestones or Risk Based Decisions.

Finally, we identified inaccuracies in the inventory data for [redacted] platform assets that were inaccurately classified in the platform inventory data. In addition, we identified [redacted] production assets in the vulnerability scan report that were missing from the platform inventory.

What TIGTA Recommended

We made five recommendations including that the Chief Information Officer should prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform; complete a Plan of Action and Milestones to document and track each overdue configuration vulnerability; and reconcile the platform asset inventory to the new inventory management system to ensure completeness and accuracy.

The IRS agreed with all five of our recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 15, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform [redacted]

This report presents the results of our review to determine the effectiveness of the General Support System [redacted] Platform systems security and operations and to determine whether the Internal Revenue Service (IRS) effectively implemented prior recommendations. This review is part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS Resources*.

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

Table of Contents

Background

The Internal Revenue Service (IRS) manages diverse and complex automated information systems which include system file servers, and local and wide area networks running various platforms to carry out its wide-ranging responsibilities. The functions and offices within the IRS depend on the confidentiality, integrity, and availability of these systems and their data to accomplish daily activities. The IRS relies on the [redacted] Platform (hereafter called the platform), one of its General Support Systems, to provide services to other federal agencies and the public. The platform provides an infrastructure to support enterprise tax administration, administrative support applications, and the Affordable Care Act.[1] The Information Technology organization has the responsibility for deploying and maintaining the hardware and software configurations for the platform.

System security requirements

Without effective security controls, the IRS's systems are vulnerable to actions taken by individuals with malicious intent. If this occurred, it could lead to the potential exposure of sensitive taxpayer data and/or damage the reputation of the IRS. The minimum system security requirements of a General Support System include monitoring for and remediation of vulnerabilities, ensuring configuration compliance, conducting a system inventory, and protecting against malicious code. According to the Internal Revenue Manual (IRM), the following activities must be completed:

- Automated security scanning of assets for inventory configuration and vulnerability data.
- Regular checks for updates to malicious code scanning tools.
- Use of IRS-approved verification or approved security monitoring systems.

Prior reporting has identified deficiencies with the platform

We have performed several audits that reviewed various elements of the platform, including:

- In February 2016, we reported that the IRS did not effectively manage the backup and restoration process for its Tier II environment.[2] This environment includes, but is not limited to, [redacted] systems.
- In May 2018, we reported that the IRS did not effectively mitigate critical and high-risk Integrated Data Retrieval System vulnerabilities.[3] These vulnerabilities also included, but were not limited to, [redacted] systems in the Tier II environment.

[1] See Appendix IV for a glossary of terms. Patient Protection and Affordable Care Act (Affordable Care Act), Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of 26 and 42 U.S.C.), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

[2] TIGTA, Report No. 2016-20-019, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* p. 8 (February 2016).

[3] TIGTA, Report No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* p. 10 (May 2018).

- In December 2018, we reported that a [redacted] migration project operated without appropriate governance leading to project delays.[4]
- In June 2019, 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.[5] These mainframes included, but were not limited to, the platform.
- In September 2021, we reported several deficiencies including insufficient vulnerability scanning and remediation and the need for improvements in the platform inventory reconciliation process, among others.[6]

Results of Review

Although All Production Servers Are Scanned for Vulnerabilities, Some Vulnerabilities Are Not Timely Remediated

Credentialed scans are performed on production servers

In September 2021, the IRS agreed with our recommendation to ensure that credentialed scans are completed on the platform servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications.[7] In February 2022, the IRS closed the recommendation stating its Cybersecurity function collaborated with the Enterprise Operations function to ensure that credentialed scans are performed on the platform servers connected to the network.

Our review confirmed that the IRS is performing credentialed scans on production servers as required. The IRM requires that information systems and hosted applications are scanned for vulnerabilities every 30 days and when new vulnerabilities potentially affecting the system or application are identified and reported. In addition, the IRM requires the IRS to implement [redacted] authorization to all information system components for selected vulnerability scanning to facilitate more thorough scanning. We found that all scanned production servers received credentialed scans.

Security vulnerabilities continue to exceed remediation time frames

In September 2021, we also reported that the IRS did not remediate vulnerabilities timely. Specifically, we identified [redacted] vulnerabilities across [redacted] unique servers exceeded the IRS policy for timely remediation. The IRS agreed to ensure that the backlog of vulnerabilities in the

[4] TIGTA, Report No. [redacted] p. 4 (December 2018).

[5] TIGTA, Report No. 2019-20-031, *Software Version Control Management Needs Improvement* p. 5 (June 2019).

[6] TIGTA, Report No. 2021-20-063, *********2******** Platform Management Needs Improvement* p. 9 (September 2021).

[7] TIGTA, Report No. 2021-20-063, *********2******** Platform Management Needs Improvement* p. 9 (September 2021).

platform was immediately resolved. In January 2022, the IRS reported that this planned corrective action had been fully implemented and closed the recommendation.

During our review, we found that the IRS had a [redacted] percent reduction of unresolved and overdue vulnerabilities when compared to the total numbers reported in September 2021. However, we continue to find security vulnerabilities that exceed remediation time frames. Our review of the vulnerability scan reports from September through November 2024 identified [redacted] vulnerabilities across [redacted] unique servers that exceeded the IRS's policy for timely remediation. Specifically, our analysis of the enterprise vulnerability report

- [redacted] known exploited vulnerabilities. Our review identified [redacted] unique vulnerability spread across [redacted] servers that exceeded the Cybersecurity and Infrastructure Security Agency established due date. Known exploited vulnerabilities are system security vulnerabilities that have been successfully exploited, as well as vulnerabilities associated with ransomware campaigns. At the time of our review, these vulnerabilities were [redacted] days overdue.
- [redacted] critical vulnerabilities. Our review identified [redacted] unique critical vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] calendar days for remediation. Critical vulnerabilities have the potential of severe impact to the organization, often resulting in unauthorized access to the device or network. These vulnerabilities ranged from [redacted] days overdue.
- [redacted] high vulnerabilities. Our review identified [redacted] unique high vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] calendar days for remediation. High vulnerabilities have the potential of significant impact to the organization, often resulting in outages or loss of confidential information. These vulnerabilities ranged from [redacted] days overdue.
- [redacted] medium vulnerabilities. Our review identified [redacted] unique medium vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] calendar days for remediation. Medium vulnerabilities have potential impact, often as part of phishing attacks or in conjunction with another vulnerability. These vulnerabilities ranged from [redacted] days overdue.
- [redacted] low vulnerabilities. Our review identified [redacted] unique low vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] calendar days for remediation. Low vulnerabilities have minimal impact, often providing information that can be used for reconnaissance. These vulnerabilities ranged from [redacted] days overdue.

Figure 1 illustrates a comparison between the current number of overdue vulnerabilities and those reported in 2021.

Figure 1: Current Overdue Vulnerabilities Versus 2021 Reported Vulnerabilities

Vulnerability Severity Level	Current Overdue Vulnerabilities	Overdue Vulnerabilities Reported in 2021
Known Exploited Vulnerabilities	[redacted]	[redacted][8]
Critical	[redacted]	[redacted]
High	[redacted]	[redacted]
Medium	[redacted]	[redacted]
Low	[redacted]	[redacted]
Totals	[redacted]	[redacted]

Source: Analysis of the platform vulnerabilities.

The IRM provides a period for remediating weaknesses discovered using automated scanning tools for vulnerability scans. The IRM also requires vulnerabilities to be prioritized by risk and remediated within certain time periods. The IRM states any exception to this policy requires the Authorizing Official to make a Risk Based Decision (RBD); or when remediation cannot be performed immediately, an identified vulnerability must be documented in a Plan of Action and Milestones (POA&M) document.

Although we continue to identify vulnerabilities that the IRS is not timely remediating, the IRS followed established policy and either correctly developed POA&Ms to track the remediation of the vulnerabilities we identified or formally accepted the risk of existing vulnerabilities.

Prior Configuration Control Weaknesses Have Been Addressed; However, the Remediation of Vulnerabilities Continues to Exceed Expected Time Frames

In September 2021, we evaluated the IRS's configuration controls and found that they were insufficient.[9] Specifically, we reported vulnerabilities on [redacted] production servers were not compliant with configuration requirements. In addition, we reported that the age of configuration vulnerabilities was not tracked. The IRS implemented a historical age tracking capability to include the last pass and last fail dates. This information is needed to properly prioritize vulnerabilities and provide the ability to monitor configuration compliance for the platform.

We also found that the platform's configuration compliance has improved. We identified [redacted] production servers were compliant.[10] The remaining [redacted] servers were not compliant due to having a [redacted] A server is compliant if the compliance score is greater than [redacted] a high configuration compliance finding.

[8] This vulnerability category was established in November 2021.

[9] TIGTA, Report No. 2021-20-063, *[redacted] Platform Management Needs Improvement* p. 6 (September 2021).

[10] The IRS's platform inventory contained [redacted] production servers. However, this inventory count was inaccurate, as discussed later this report.

Configuration vulnerabilities are not remediated within expected time frames

During our review, we found that the IRS did not remediate vulnerabilities within the expected time frames. According to the IRM, vulnerabilities should be prioritized and those with the highest risk should be remediated first. Further, configuration vulnerabilities should be remediated within pre-determined time frames based on the risk level of each vulnerability, as shown in Figure 2.

Figure 2: Vulnerability Severity Rating Scale and Remediation Time Frames

Vulnerability Severity Level	Expected Remediation Time Frame
High	90 days
Medium	120 days
Low	180 days

Source: The IRM.

Our review of the configuration scan reports for January 2025 found [redacted] configuration vulnerabilities across [redacted] unique servers that exceeded the IRS's policy for timely remediation. Specifically, we found:

- [redacted] medium configuration vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] days for remediation. These vulnerabilities ranged from [redacted] days overdue.
- [redacted] low configuration vulnerabilities spread across [redacted] servers that exceeded the IRS policy of [redacted] days for remediation. These vulnerabilities ranged from [redacted] days overdue.

Some of these vulnerabilities exist on servers which support the processing of tax information, IRS critical business processes, and mission essential functions. For example, [redacted] all reside on servers with configuration vulnerabilities. These systems are responsible for receiving and processing [redacted] identifying [redacted] compliance, and [redacted] The IRS stated these were not timely remediated because it does not have enough qualified personnel to remediate the platform and must prioritize remediating the critical and high-risk configuration compliance vulnerabilities.

In June 2025 the acting Chief Information Officer stated that more than 2,000 information technology employees had been separated since January 2025. With the IRS's recent workforce reductions, prioritizing its resources is critical to ensure that vulnerabilities are addressed. Configuration vulnerabilities that are not timely remediated could provide an individual with malicious intent the opportunity to access and control the IRS's servers.

Recommendation 1: The Chief Information Officer should prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform.

Management's Response: The IRS agreed with this recommendation and will prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform.

Inconsistent guidance resulted in undocumented remediation delays

We also found that the IRS did not have a POA&M or an RBD for the [redacted] configuration compliance vulnerabilities that were not remediated timely. Further review of the IRS's requirements identified inconsistencies between IRS policies and Standard Operating Procedures. For example:

- The IRM requires the information system owner to provide a justification, in a POA&M, when a remediation of a vulnerability is delayed due to agency needs.
- The IRS's *Vulnerability Management Standard Operating Procedures* note that a POA&M or an RBD should be used to document and track vulnerabilities that are not remediated within the required time frame.
- In contrast to the above bullets, the IRS's *Enterprise FISMA Plan of Action and Milestones (POA&M) Standard Operating Procedure (SOP),* Version 12 states that IRS business units have the option to not officially create POA&Ms for medium and low vulnerabilities.

The IRS did not have clear and consistent guidance to ensure that POA&Ms or RBDs for vulnerabilities were completed. The misalignment between policies and procedures may result in confusion and lead to inconsistent decisions on documenting remediation activities. In addition, if the IRS does not track all vulnerabilities, there is a possibility some of them will not be remediated.

The Chief Information Officer, should:

Recommendation 2: Complete POA&Ms and/or RBDs to document and track the [redacted] overdue configuration compliance vulnerabilities.

Management's Response: The IRS agreed with this recommendation and will ensure that POA&Ms and/or RBDs are completed to document and track the [redacted] overdue configuration compliance vulnerabilities.

Recommendation 3: Ensure that the Standard Operating Procedures and IRM reflect consistent guidance regarding the requirements and timing of POA&Ms and/or RBDs.

Management's Response: The IRS agreed with this recommendation and will ensure that the Standard Operating Procedures and policy (via Interim Guidance memo) are updated to reflect consistent guidance regarding the requirements and timing of POA&Ms and/or RBDs.

The IRS Implemented [redacted] but Some Systems Are Still [redacted]

In March 2023, we reported that the IRS did not have [redacted] for some of the platform's servers and that these were not effectively tracked with a POA&M.[11] The IRS agreed to develop, test, and implement an automated [redacted] application on all platform servers.

[11] TIGTA, Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* pp. 5-6 (March 2023).

We compared the November 2024 platform inventory with the February 2025 [redacted] scan report and confirmed that the IRS has implemented [redacted] for the platform servers. Specifically, we found that [redacted] production servers had compliant client software installed and were scanned [redacted] with updated virus definitions.[12] Of the remaining [redacted] production servers:

- [redacted] did not have malicious code protection installed because their operating systems were incompatible with the [redacted] solution deployed by the IRS.
- [redacted] began the retirement process (*i.e.*, preparing to remove the server from service) in January and February 2025. Therefore, it is reasonable that the IRS did not have [redacted] installed.

The IRS did not have a documented RBD or POA&M for the [redacted] servers that did not have [redacted] installed. The IRM states that an RBD can be used to document when meeting a requirement is not operationally feasible. IRS management acknowledged that the failure to develop an RBD was an oversight. If a system lacks [redacted] it becomes highly vulnerable to attacks, potentially leading to data theft, system disruption, identity theft, financial losses, and reputational damage.

Recommendation 4 (Conversation): The Chief Information Officer should develop and approve an RBD or POA&M for deviating from the requirement to employ [redacted] for all systems.

Management's Response: The IRS agreed with this recommendation and formally accepted the risk of operating [redacted] production servers on the platform without [redacted] by completing and approving a RBD.

The Platform Inventory Is Inaccurate

The platform provides the infrastructure for information system components used by the IRS. The IRS's internal guidelines and the National Institute of Standards and Technology require the IRS to develop and document an accurate inventory of the platform. This inventory should include all components of a system and not include duplicate entries or entries for components assigned to another system.[13]

Our review of the platform inventory data identified reporting inaccuracies. The initial platform inventory contained [redacted] production servers deemed available and in use. However, our review found [redacted] platform assets that were inaccurately classified in the platform inventory data.[14] Specifically, we found:

- [redacted] assets incorrectly classified as servers. The IRS stated these were appliances.
- [redacted] assets incorrectly recorded as "in use" instead of "retired" or "in stock."

[12] The IRS's platform inventory contained [redacted] production servers. However, this inventory count was inaccurate, as discussed later this report.

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

[14] Assets include both servers and appliances.

- [redacted] assets incorrectly designated as "available," instead of "in build" status (*i.e.*, ready to be deployed).

Due to these reporting inaccuracies, we removed the [redacted] platform assets from our review, leaving a total of [redacted] production servers to further evaluate. In addition, we found [redacted] production assets listed in the vulnerability scan report that were missing from the platform inventory. Inaccurate and misclassified inventory records can lead to these servers being excluded from having their vulnerabilities prioritized and remediated.

When we notified IRS management of the platform inventory data inaccuracies, they stated the inaccuracies resulted from a recent migration to a new inventory management system. In addition, management officials from the Cybersecurity function's Security Operations and Standards Division stated they updated the platform inventory to correct the classification of the [redacted] assets we identified. In February 2025, the IRS provided us with an updated inventory, and we confirmed it was corrected.

Recommendation 5: The Chief Information Officer should reconcile the platform asset inventory to the new inventory management system to ensure its completeness and accuracy.

Management's Response: The IRS agreed with this recommendation and will reconcile the platform asset inventory to the new inventory management system to ensure its completeness and accuracy.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this review were to determine the effectiveness of the General Support System [redacted] Platform systems security and operations and to determine whether the IRS effectively implemented prior recommendations. To accomplish these objectives, we:

- Determined whether the IRS effectively implemented the closed recommendation to ensure the backlog of vulnerabilities in the platform environment were immediately resolved and a process to do so on an ongoing basis has been effectively implemented. We also reviewed vulnerability scan reports to determine whether the closed prior recommendation to ensure that credentialed scans are completed on the platform servers to determine the full extent of vulnerabilities affecting the installed operating systems and applications has been effectively implemented.
- Determined whether the configuration management process is effectively documented and managed by obtaining and analyzing configuration compliance reports. We also determined whether the IRS has effectively implemented prior recommendations by evaluating whether the closed recommendations to provide age tracking capability for vulnerabilities detected by the configuration scanning tool were properly implemented.
- Determined whether [redacted] are effective for the platform's environment by obtaining and analyzing [redacted] reports to determine the scan frequency and [redacted]
- Determined whether the platform inventory was accurate by comparing the official inventory to the [redacted] security vulnerability, and configuration scan reports.

Performance of This Review

This review was performed with information obtained from the Cybersecurity Architecture and Implementation function located in [redacted] Maryland; the Information Technology organization's Computer Security Incident Response Center located in [redacted] Tennessee; Security Risk Management function located in [redacted] Texas; and the Enterprise Operations, Security Operations and Standards Division located in [redacted] West Virginia, during the period September 2024 through March 2025. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Data Validation Methodology

We performed tests to assess the reliability of the data obtained from the Security Information and Event Management tool and the platform inventory system. We evaluated the data by: 1) interviewing IRS personnel knowledgeable about the data; 2) ensuring that the information was legible and contained alphanumeric characters; 3) reviewing required data elements; and

4) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data. We determined that the data from the Security Information and Event Management tool and official inventory were sufficiently reliable for purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: National Institute of Standards and Technology guidance and IRM policies. We evaluated these controls by interviewing IRS subject matter experts and analyzing [redacted] configuration compliance, and vulnerability reports.

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; [redacted] unique servers have [redacted] medium and [redacted] low severity levels that exceeded the IRS policy for timely remediation (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We reviewed the configuration compliance scan reports for January 2025 and found [redacted] configuration vulnerabilities across [redacted] unique servers exceeded the IRS policy for timely remediation. We found that this included [redacted] medium configuration vulnerabilities and [redacted] low configuration vulnerabilities.

Type and Value of Outcome Measure:

Protection of Resources – Potential; [redacted] configuration compliance vulnerabilities are not being tracked with a POA&M or RBD (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We determined that the IRS did not have POA&Ms or RBDs for the [redacted] configuration compliance vulnerabilities that were not remediated timely.

Type and Value of Outcome Measure:

Protection of Resources – Potential; [redacted] production servers did not have [redacted] installed (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

We compared the official inventory dated November 2024 with the [redacted] report dated February 2025 and found [redacted] servers did not have [redacted] installed.

Type and Value of Outcome Measure:

Reliability of Information – Potential; [redacted] platform assets were either not accounted for or had the wrong status in the official inventory (see Recommendation 5).

Reliability of Information – Actual; [redacted] platform assets were incorrectly identified as servers (see Recommendation 5).

Methodology Used to Measure the Reported Benefit:

The platform inventory originally contained [redacted] production servers deemed available and in use. Our review found [redacted] platform assets that were inaccurately classified. Specifically, we found

[redacted] assets that were either not accounted for or had the wrong status (*i.e.*, in use or available). In addition, we found [redacted] assets identified as servers instead of appliances. During our audit, management officials from the Cybersecurity function's Security Operations and Standards Division correctly updated these [redacted] assets to appliances.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

August 5, 2025

MEMORANDUM FOR DIANA M. TENGESDAL
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Chief Information Officer
Courtney M. Williams
Digitally signed by Courtney M. Williams
Date: 2025.08.05 22:20:53 -04'00'

SUBJECT: Draft Audit Report – The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform [redacted]

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. We agree that the IRS should prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform, complete a Plan of Action and Milestones to document and track each overdue configuration vulnerability, and reconcile the platform asset inventory to the new inventory management system to ensure completeness and accuracy.
The IRS is committed to fully and effectively implement and document all agreed upon corrective actions. The IRS's Enterprise Audit Management has instituted regular process reviews that ensure agreed upon corrective actions are implemented in a timely manner and will continue to conduct rigorous post-implementation reviews to ensure these actions are sustained.

We agree with the Treasury Inspector General for Tax Administration's five recommendations and have already begun responding. Our corrective action plan for the five recommendations and four outcome measures identified in the report is attached.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (304) 616-1818, or a member of your staff may contact Houman Rasouli, Coordinating Director, Cybersecurity, at (202) 317-6606.

Attachment

Attachment

[redacted] The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform

Recommendations

RECOMMENDATION 1: The Chief Information Officer should prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will prioritize and resolve the backlog of configuration compliance vulnerabilities in the platform.

IMPLEMENTATION DATE: March 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should complete POA&Ms and/or RBDs to document and track the [redacted] overdue configuration compliance vulnerabilities.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will ensure that POA&Ms and/or RBDs are completed to document and track the [redacted] overdue configuration compliance vulnerabilities.

IMPLEMENTATION DATE: April 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 3: The Chief Information Officer should ensure that the Standard Operating Procedures and IRM reflect consistent guidance regarding the requirements and timing of POA&Ms and/or RBDs.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will ensure that the Standard Operating Procedures and policy (via Interim Guidance memo) are updated to reflect consistent guidance regarding the requirements and timing of POA&Ms and/or RBDs.

IMPLEMENTATION DATE: November 15, 2025

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

Attachment

[redacted] The IRS Made Some Progress Implementing Effective Protection for the [redacted] Platform

RECOMMENDATION 4: The Chief Information Officer should develop and approve an RBD or POA&M for deviating from the requirement to employ [redacted] for all systems.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The IRS formally accepted the risk of operating [redacted] production servers on the platform without [redacted] by completing and approving a Risk-Based Decision.

IMPLEMENTATION DATE: September 15, 2025

RESPONSIBLE OFFICIAL(S): Coordinating Director, Cybersecurity

RECOMMENDATION 5: The Chief Information Officer should reconcile the platform asset inventory to the new inventory management system to ensure its completeness and accuracy.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer will reconcile the platform asset inventory to the new inventory management system to ensure its completeness and accuracy.

IMPLEMENTATION DATE: February 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

Appendix IV

Glossary of Terms

Term	Definition
Appliance	A computing device that provides predefined services and has its underlying operating software hidden beneath an application specific interface.
Credentialed Scan	A type of security vulnerability assessment that involves providing the scanning tool with valid login credentials to the targeted systems.
Critical Vulnerabilities	Critical vulnerabilities have the potential of severe impact to the organization, often resulting in unauthorized access to the device or network
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
High Vulnerabilities	High vulnerabilities have the potential of significant impact to the organization, often resulting in outages or loss of confidential information.
In Build	This is used to identify an asset that is being readied for deployment.
In Stock	Refers to equipment that is not in production and may be in storage pending installation, deployment, or disposal.
In Use	Refers to equipment assigned, deployed, installed, and in production.
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	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.
Known Exploited Vulnerabilities	A compilation of documented security vulnerabilities that have been successfully exploited, as well as vulnerabilities associated with ransomware campaigns.
Low Vulnerabilities	Low vulnerabilities have minimal impact, often providing information that can be used for reconnaissance
Medium Vulnerabilities	Medium vulnerabilities have potential impact, often as part of phishing attacks or in conjunction with another vulnerability.
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.

Term	Definition
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
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.
Retirement Process	The process of removing an information technology asset from service. This process includes discontinuing monitoring and patching activities and preparing the asset for removal from the network.
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 Information and Event Management	A security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.
Tier I	Supercomputers and mainframe hardware and software, including peripheral subsystems used in a mainframe system environment.
Tier II	The Tier II environment consists of non-mainframe servers. These servers run various operating systems. The servers may also operate as database, web, e-mail, and file servers, and provide a host of other important functions supporting the IRS network infrastructure.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system to determine if and where a system can be exploited or threatened. It 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

IRM	Internal Revenue Manual
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones
RBD	Risk Based Decision
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

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

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