TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement

September 26, 2024

Report Number: 2024-200-057

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

HIGHLIGHTS: Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement

Final Audit Report issued on September 26, 2024 **Report Number 2024-200-057**

Why TIGTA Did This Audit

The IRS uses General Support Systems (GSS) that are an interconnected set of information resources under the same direct management control which shares common functionality. The IRS also uses Major Applications that require special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

The IRS uses an asset and vulnerability repository to collect and index data and to assist business units in detecting unauthorized intrusions and privileged access abuse. The IRS also uses the repository to manage vulnerabilities and configuration compliance.

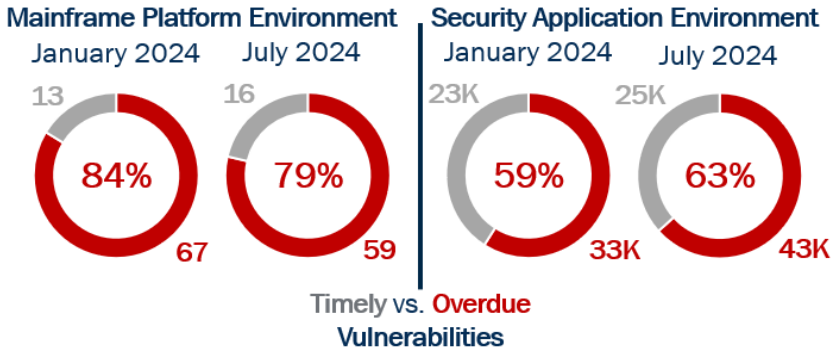
This audit was initiated to review the vulnerability and configuration compliance of one GSS and one Major Application.

Impact on Tax Administration

Federal and organizational policies require the IRS to identify and timely remediate vulnerabilities on its information technology assets and to maintain compliance with configuration management and monitoring standards. Unresolved vulnerabilities and noncompliant asset configurations increase risk to the overall security of IRS assets.

What TIGTA Found

TIGTA reviewed one GSS and one Major Application for this audit: a Mainframe Platform Environment and a Security Application Environment. In January 2024, the Mainframe Platform Environment had 80 vulnerabilities that were open and unresolved. Of the 80 vulnerabilities, 67 were overdue: 15 had a Critical Risk, 30 had a High Risk, and 22 had a Medium Risk. The remaining 13 vulnerabilities were open but not overdue. The Security Application Environment had 56,537 open and unresolved vulnerabilities. Of these, 33,366 were overdue: 2,048 had a Critical Risk, 13,558 had a High Risk, 15,452 had a Medium Risk, and 2,308 had a Low Risk. The remaining 23,171 vulnerabilities were open but not overdue. TIGTA conducted a follow-up in July 2024 to determine the status of the vulnerabilities.



Internet Protocol addresses were not always assigned to the correct environments. Specifically, the IRS did not properly assign 123 Internet Protocol addresses to the Mainframe Platform Environment and 62 Internet Protocol addresses to the Security Application Environment.

Further, 99 Internet Protocol addresses of the Security Application Environment assets were outside of the assigned range. Lastly, a total of 743 assets used noncompliant configurations across both environments.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer should: 1) timely remediate or mitigate all vulnerabilities in accordance with IRS policies; 2) ensure that assets are assigned to an established group; 3) ensure that systems are in place to reconcile duplicate accounting of assets; 4) reconcile assets to reflect the operating environment; 5) evaluate temporary repositories to establish ownership of assets; and 6) resolve configuration compliance settings in accordance with Federal and IRS policies.

The IRS agreed with five recommendations and plans to review vulnerability remediation processes, implement zero trust best practices to remove physical assets not properly documented, collaborate with authorizing officials to reconcile assets, and ensure that configuration settings meet Federal and IRS policies. The IRS disagreed with reconciling Internet Protocol addresses to assets to reflect the operating environment. TIGTA responded to the disagreement.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 26, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement (Audit No.: 2024200004)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) effectively assigned information technology assets and addressed security vulnerability and configuration issues on one General Support System and one Major Application. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources*.

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

Table of Contents

Background

The Internal Revenue Service (IRS) uses General Support Systems (GSS) that are an interconnected set of information resources under the same direct management control which shares common functionality. These systems typically include hardware, software, information, data, applications, communications, and people.[1] In addition, the IRS uses Major Applications that require special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. System owners must ensure that the system components are accurately recorded, and system vulnerabilities are identified and remediated timely.

The IRS leverages the asset and vulnerability repository to collect and generate audit records for security-related events.[2] The asset and vulnerability repository assists individual business units and projects to detect unauthorized intrusions and privileged access abuse. The asset and vulnerability repository collects and indexes machine data from physical, virtual, or cloud environments that can be used for security, configuration compliance, fraud detection, infrastructure, operational management, and for application delivery and quality assurance. The repository currently tracks 21 different GSSs and Major Applications and identifies a point of contact and responsible organization for each system. Included in the repository are vulnerability reports for temporary (a place holder for new assets added to the network that do not have a predefined GSS) and unknown (assets in which the GSS field is blank) information technology assets.

Results of Review

Assets Contained Overdue and Unresolved Vulnerabilities

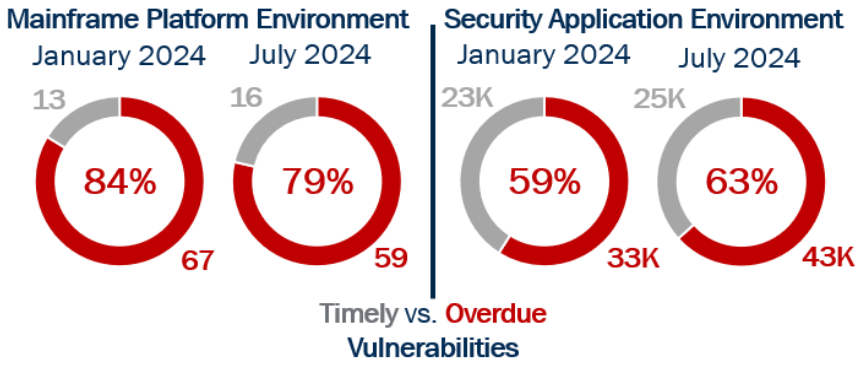
We reviewed the January and July 2024 vulnerability reports for a GSS, Mainframe Platform Environment, and a Major Application, Security Application Environment. The vulnerability report includes identifiers to categorize the status of the vulnerability resolution such as the severity of the vulnerability and the number of days a vulnerability has affected an asset.

Figure 1 compares and summarizes the number of overdue vulnerabilities in January and July 2024 and provides the percentages of overdue vulnerabilities.

[1] Internal Revenue Manual (IRM), 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance* (July 26, 2024).

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

Figure 1: Timely and Overdue Vulnerabilities



Source: Treasury Inspector General for Tax Administration's (TIGTA) review of vulnerability reports from the IRS asset and vulnerability repository.

The Mainframe Platform Environment January 2024 vulnerability report identified 80 unresolved vulnerabilities across 18 assets. The vulnerabilities had the following timeliness and severity rating characteristics:

- 67 (84 percent) vulnerabilities were overdue, *i.e.*, not mitigated within required time frames, affecting 18 assets. Of these vulnerabilities:
  - 15 (22 percent) are Critical Risk.
  - 30 (45 percent) are High Risk.
  - 22 (33 percent) are Medium Risk.
- 13 (16 percent) vulnerabilities were timely, *i.e.,* within the time frame allowed for mitigation.

In July 2024, we conducted a follow-up assessment of the Mainframe Platform Environment vulnerability report and found that 75 vulnerabilities were unresolved across 17 assets. The vulnerabilities had the following timeliness and severity rating characteristics:

- 59 (79 percent) vulnerabilities were overdue, *i.e.*, not mitigated within required time frames affecting 12 assets. Of these vulnerabilities:
  - 4 (7 percent) are Critical Risk.
  - 27 (46 percent) are High Risk.
  - 28 (47 percent) are Medium Risk.
- 16 (21 percent) vulnerabilities were timely, *i.e.*, within the time frame allowed for mitigation.

Enterprise Operations personnel are aware of these overdue vulnerabilities and are working to mitigate the risk through a Plan of Action and Milestones. However, we found that all Plan of Action and Milestones mitigation documents specific to the Mainframe Platform Environment were created after the start of our planning for this audit in October 2023.

We also reviewed the vulnerability and asset repository reports to determine the severity level of all overdue vulnerabilities for the Mainframe Platform Environment, which are presented in Figure 2 and Figure 3 for January and July 2024, respectively.

Figure 2: Number and Percentage of Vulnerabilities by Severity Rating for the Mainframe Platform Environment for January 2024

GSS	CRITICAL	HIGH	MEDIUM	LOW
Timely	1	0	12	0
Overdue	15	30	22	0
Total Vulnerabilities	16	30	34	0

Source: TIGTA's review of vulnerability reports from the IRS asset and vulnerability repository.

Figure 3: Number and Percentage of Vulnerabilities by Severity Rating for the Mainframe Platform Environment for July 2024

GSS	CRITICAL	HIGH	MEDIUM	LOW
Timely	0	16	0	0
Overdue	4	27	28	0
Total Vulnerabilities	4	43	28	0

Source: TIGTA's review of vulnerability reports from the IRS asset and vulnerability repository.

We also reviewed the January 2024 vulnerability report for the Security Application Environment and identified 56,537 unresolved vulnerabilities across 580 assets. The vulnerabilities had the following timeliness and severity rating characteristics:

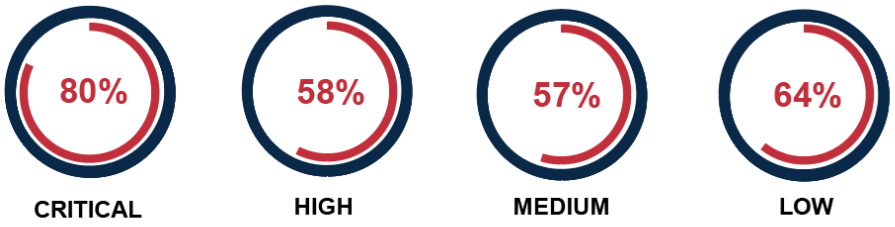
- 33,366 (59 percent) vulnerabilities were overdue, *i.e.*, not mitigated within required time frames affecting 569 assets. Of these vulnerabilities:
  - 2,048 (6 percent) are Critical Risk.
  - 13,558 (41 percent) are High Risk.
  - 15,452 (46 percent) are Medium Risk.
  - 2,308 (7 percent) are Low Risk.
- 23,171 (41 percent) vulnerabilities were timely, *i.e.*, within the time frame allowed for mitigation.

In July 2024, we completed a follow-up assessment of the Security Application Environment vulnerability report and found a total of 68,355 unresolved vulnerabilities across 581 assets. The vulnerabilities had the following timeliness and severity rating characteristics:

- 43,290 (63 percent) vulnerabilities were overdue, *i.e.,* not mitigated within required time frames, affecting 570 assets. Of these vulnerabilities:
  - 1,822 (4 percent) are Critical Risk.
  - 23,735 (55 percent) are High Risk.
  - 16,749 (39 percent) are Medium Risk.
  - 984 (2 percent) are Low Risk.
- 25,065 (37 percent) vulnerabilities were timely, *i.e.*, within the time frame allowed for mitigation.

We also reviewed the vulnerability and asset repository reports to determine the severity level of all overdue vulnerabilities for the Security Application Environment, which are presented in Figure 4 and Figure 5 for January and July 2024, respectively.

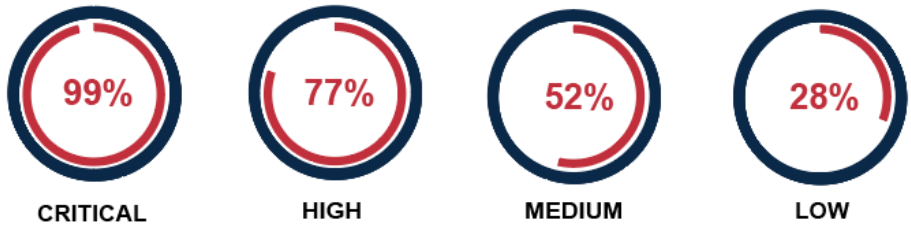
Figure 4: Number and Percentage of Vulnerabilities by Severity Rating for the Security Application Environment for January 2024



	CRITICAL	HIGH	MEDIUM	LOW
Timely	503	9,874	11,492	1,302
Overdue	2,048	13,558	15,452	2,308
Total Vulnerabilities	2,551	23,432	26,944	3,610

Source: TIGTA's review of vulnerability reports from the IRS asset and vulnerability repository.

Figure 5: Number and Percentage of Vulnerabilities by Severity Rating for the Security Application Environment for July 2024



MAJOR APPLICATION	CRITICAL	HIGH	MEDIUM	LOW
Timely	22	6,908	15,610	2,525
Overdue	1,822	23,735	16,749	984
Total Vulnerabilities	1,844	30,643	32,359	3,509

Source: TIGTA's review of vulnerability reports from the IRS asset and vulnerability repository.

Cybersecurity and Enterprise Operations function personnel follow National Institute of Standards and Technology and Internal Revenue Manual (IRM) policies for vulnerability remediation to safeguard the Mainframe Platform Environment and the Security Application Environment.[3] We found that policies outline specific metrics for evaluating risk and vulnerability resolution. If a vulnerability cannot be effectively remediated, the system's owner is required to document the vulnerability in a Risk-Based Decision or Plan of Action and Milestones. However, the vulnerability remediation process is not always effective.

IRM policy states that the IRS must monitor and scan for vulnerabilities in the system and hosted applications. The IRS must also analyze vulnerability scan reports and results and remediate vulnerabilities in accordance with response times for the severity level/rank of the vulnerability. IRS vulnerabilities must be prioritized for remediation based on risk, and vulnerabilities with the highest risk must be remediated first. Once prioritized, the IRS must remediate vulnerabilities based on time frames defined in Figure 6.

Figure 6: Remediation Timelines

Risk Level	Remediate Vulnerability
Critical	•Internet Accessible systems identified on Department of Homeland Security, Cyber Hygiene Reports = 15 Days. •All other systems = 30 Days.
High	•Internet Accessible systems identified on Department of Homeland Security, Cyber Hygiene Reports = 30 Days. •High Value Assets = 60 Days. •All other systems = 90 Days.
Medium	•120 Days.
Low	•180 Days.

Source: IRM 10.8.1.

Cybersecurity personnel confirmed that the unresolved vulnerabilities are the result of a transition from one vulnerability scanning tool to another. The transition to the new tool resulted in more robust scanning and an overall increase in the volume of identified vulnerabilities that they have not addressed. Enterprise Operations and Cybersecurity personnel agree that vulnerabilities persist. TIGTA previously reported on the IRS not timely remediating vulnerabilities.[4] The existence of unresolved vulnerabilities increases the risk to the overall security of IRS assets.

Recommendation 1: The Chief Information Officer should timely remediate or mitigate all vulnerabilities in accordance with IRS policies.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will review vulnerability remediation practices and processes to

[3] National Institute of Standards and Technology, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020) and IRM, Section 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 2023).

[4] TIGTA, Report No. 2023-20-048, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk* (Aug. 2023) and TIGTA, Report No. 2022-20-006, *Vulnerability Scanning and Remediation Processes Need Improvement* (Dec. 2021).

identify gaps that would prevent the process from working in an effective manner. The IRS will close these gaps and reduce vulnerability percentages by 50 percent.

Assets Were Not Assigned to the Appropriate General Support System or Major Application

The IRS has an established process in place for asset assignment. We met with Enterprise Operations and User and Network Services function personnel responsible for the asset assignment process of the Mainframe Platform Environment. The group follows a predetermined process in which asset control begins before an asset arrives at an IRS facility. According to Mainframe Platform Environment personnel, once an asset arrives on-site, Enterprise Operations personnel verify the serial number to confirm it is the correct asset. Next, a diagnostic check is performed, and an implementation date is established using a prescribed Change Management Process. Finally, the device is placed in a temporary GSS until the implementation date when the device is moved into a permanent GSS group. The process includes the collection and maintenance of numerous forms and documents.

We also met with Cybersecurity and User and Network Services personnel responsible for the asset assignment process of the Security Application Environment. The IRS follows Federal Information Security Management Act Master Inventory Standard Operating Procedures for adding an asset to an existing system boundary. These procedures include maintaining milestones throughout the process. The milestones include documented approval from an Authorizing Official and an Authority to Operate approval.

However, we found that the Mainframe Platform Environment and Security Application Environment asset assignment processes are not always effective. TIGTA previously reported on IRS asset allocation and management concerns.[5]

Individual assets were in multiple vulnerability reports

We collected 26 different data files directly from the IRS's asset and vulnerability repository. The files included asset data from vulnerability reports for all available GSS and Major Applications. We reviewed the reports and found the Security Application Environment had 69 assets that were also included in two other GSS vulnerability reports. According to IRS personnel, the unique nature of the Security Application Environment's computing environment causes cybersecurity tools and appliances to function across different GSS and Major Application boundaries. Specific examples include Virtual Machines and network security devices that help to control IRS access to the Internet.

We also reviewed the Internet Protocol (IP) addresses assigned to the Mainframe Platform Environment and Security Application Environment. We obtained a list of 6,107 IP addresses assigned to the Mainframe Platform Environment and compared it to the IP addresses of the assets identified in the temporary and unknown GSS vulnerability reports and found:

- 8 IP addresses on the temporary GSS vulnerability report are included in the Mainframe Platform Environment.

[5] TIGTA, Report No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).

- 115 IP addresses on the unknown GSS vulnerability report are included in the Mainframe Platform Environment.

In addition, we obtained a list of 5,334 IP addresses assigned to the Security Application Environment and compared it to the IP addresses of the assets identified in the temporary and unknown GSS vulnerability reports and found:

- 3 IP addresses on the temporary GSS vulnerability report are included in the Security Application Environment.
- 59 IP addresses on the unknown GSS vulnerability report are included in the Security Application Environment.

IRS management states that the IP address range assigned by User and Network Services is not a significant factor in the creation and management of information technology assets. However, the IRM states that components of Major Applications and systems do not include duplicate accountings of components or components assigned to any other system.

Discussion with IRS executive management in Cybersecurity, Enterprise Operations, and User and Network Services verified that the IRS inventory system has limitations to the identification of assets. As a result, when an asset cannot be reconciled due to this limitation, it will be placed into the temporary or unknown repositories. The IRS is in process of migrating to a new system that will have more robust capabilities and resolve the issue of items being incorrectly assigned to temporary and unknown repositories. Until the new system is functional, assets found in more than one GSS or Major Application calls into question the overall accountability for asset assignment.

The Chief Information Officer should:

Recommendation 2: Ensure that systems are in place to reconcile the temporary and unknown repositories to verify that assets are assigned to an established group.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will take steps to implement zero trust best practices to remove the physical assets across the network that are not properly documented across a taxonomy.

Recommendation 3: Ensure that systems are in place to reconcile duplicate accounting of assets in the repository.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will collaborate with all authorizing officials on their duplicate assets and respective Federal Information Security Modernization Act boundaries and reconcile assets with the appropriate business units.

The Major Application vulnerability reports contained assets with an IP address outside the assigned range

The Security Application Environment has assets with IP addresses outside of its assigned address range. We compared the Security Application Environment's address range against the Security Application Environment vulnerability report and found 99 unique IP addresses that are outside of its assigned range. The IRM requires that mechanisms be used to help maintain the currency, completeness, and accuracy of IRS system components.

While IRS management believes the IP address range is not a significant factor in the creation and management of information technology assets, the IRM states that components or Major Applications and systems should not include components assigned to any other system. Vulnerability reports with assets assigned outside the prescribed range make it difficult to effectively manage and control the environment using that unique identifier.

Recommendation 4: The Chief Information Officer should reconcile assets to reflect the operating environment.

Management's Response: The IRS disagreed with this recommendation. The management of IP addresses is not tied to reconciliation of a specific boundary or technology. IP addresses are assigned in blocks which can be misleading since they are assigned as needed.

Office of Audit Comment: By disagreeing with our recommendation, the IRS is in violation of its own policy. The Major Application was assigned a specific IP address range for its assets. The IRM requires that mechanisms be used to help maintain the accuracy of IRS system components.

Assets were not assigned to any permanent GSS or Major Application

We found seven assets listed on both the temporary and unknown GSS vulnerability reports. These assets merit special attention because the temporary report is a placeholder for assets recently added to the network without having a predefined GSS group. The unknown repository is for assets in which the GSS field is blank. IRS policy requires that Major Applications and systems must contain inventory data such as platform and type and specify the GSS or Major Application the data belong to.

IRS management stated that upon review of these seven assets, they belong to a specific application that is in the process of being retired. This explanation emphasizes the shortcomings of the existing tracking process. Having assets assigned to both a temporary place holder and a catch all repository for assets with missing GSS data significantly increases the risk of asset compromise due to management being unfamiliar with the needs of those assets.

Management Action: The IRS determined the seven assets belong to the Enterprise Systems Domain, and personnel removed the assets from the temporary and unknown vulnerability reports. On April 17, 2024, the audit team obtained copies of the temporary and unknown vulnerability reports and verified that no co-located assets were listed.

Recommendation 5: The Chief Information Officer should evaluate the temporary and unknown repositories to establish ownership of assets.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will collaborate with all authorizing officials on their temporary repositories and reconcile assets with the appropriate business units.

Assets Were Not Properly Configured

We found that the Mainframe Platform Environment and the Security Application Environment follow enterprise-wide policies in place to maintain compliance with National Institute of Standards and Technology and IRM requirements related to configuration management and monitoring.[6] Cybersecurity and Enterprise Operations personnel have implemented steps for continuously monitoring and controlling asset compliance metrics. However, the Mainframe Platform Environment and the Security Application Environment do not remain compliant. TIGTA reported previously on the status of configuration scans.[7]

We collected configuration data for the Mainframe Platform Environment and the Security Application Environment and compared it to files generated by the Cybersecurity and Enterprise Operations functions to verify that IRS personnel are accurately tracking configurations of noncompliant assets. IRS staff responsible for the Mainframe Platform Environment configuration management differentiate devices into three operating system categories: Operating System 1, Operating System 2, and Operating System 3.

We reviewed the Mainframe Platform Environment configuration compliance report from February 28, 2024, and found that 68 total assets were being tracked for configuration compliance. Of these 68 total assets:

- 23 (34 percent) belonged to Operating System 1.
- 5 (7 percent) belonged to Operating System 2.
- 40 (59 percent) belonged to Operating System 3.

According to the configuration compliance report, the assets belonging to Operating Systems 1 and 2 were noncompliant, while the assets in Operating System 3 were compliant. Therefore, 28 (41 percent) of 68 assets were noncompliant while 40 (59 percent) of the 68 assets were compliant. According to the Dashboard User Guide, configuration compliance is achieved when a system reaches a weighted compliance score of 90 percent or higher and does not include any high-severity findings. We found that:

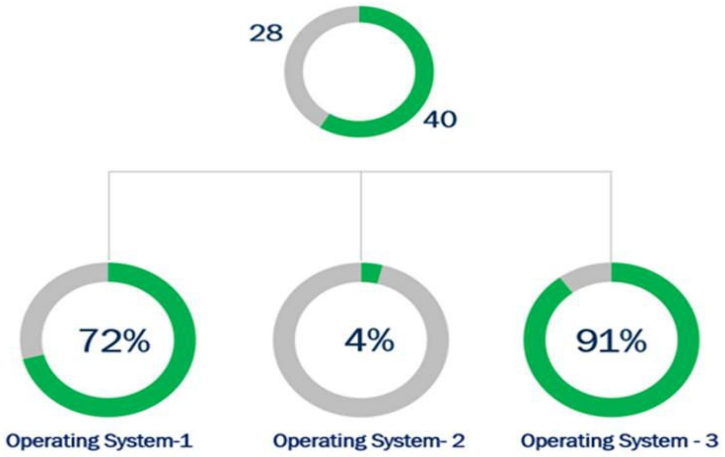
- Operating System 1 - assets were noncompliant with an overall compliance score of 72 percent.
- Operating System 2 - assets were noncompliant with an overall compliance score of 4 percent.
- Operating System 3 - assets were compliant with an overall compliance score of over 91 percent.

Figure 7 shows the overall compliance for the Mainframe Platform Environment assets followed by the overall score for each operating system for the review completed on February 28, 2024.

[6] IRM, 2.150.1, *Configuration Management Policy* (Apr. 1, 2024).

[7] TIGTA, Report No. 2022-20-050, *Mainframe Platform Configuration Compliance Controls Need Improvement* (Sept. 2022) and TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

Figure 7: Mainframe Platform Environment Compliance Scores for February 2024



Source: TIGTA's review of configuration compliance reports from the IRS asset and vulnerability repository.

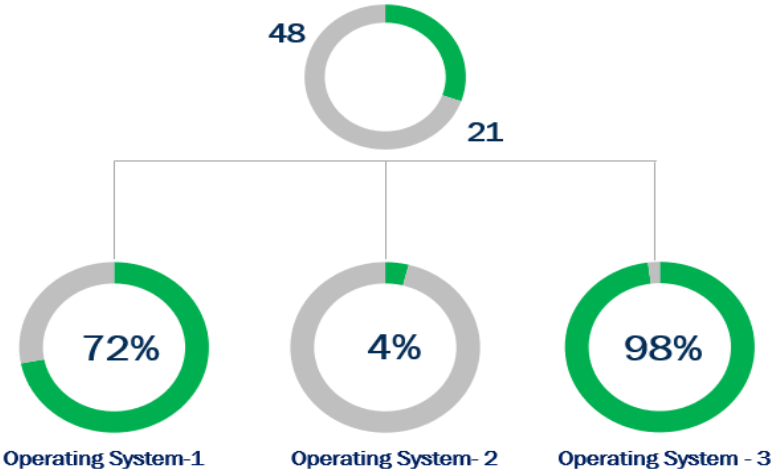
A follow-up review of the Mainframe Platform Environment configuration compliance report from July 25, 2024, found that 69 total assets were being tracked for configuration compliance. According to the configuration compliance report, 28 (41 percent) of 69 assets from Operating Systems 1 and 2 was noncompliant, and 20 (29 percent) assets from Operating System 3 were noncompliant. The remaining 21 (30 percent) of 69 assets from Operating System 3 were compliant. We found only a slight change in overall compliance from February 2024 to July 2024:

- Operating System 1 - assets were noncompliant with an overall compliance score of 72 percent.
- Operating System 2 - assets were noncompliant with an overall compliance score of 4 percent.
- Operating System 3 - assets were compliant with an overall score of over 98 percent.[8]

Figure 8 shows the overall compliance for the Mainframe Platform Environment assets followed by the overall score by operating system for the review completed five months later, on July 25, 2024.

[8] Compliant assets have a weighted compliance score of 100 percent, and noncompliant assets have a weighted compliance score of 96 percent. An asset can have a weighted compliance score of over 90 percent and still be considered noncompliant if any findings are high severity.

Figure 8: Mainframe Platform Environment Compliance Scores for July 2024



Source: TIGTA's review of configuration compliance reports from the IRS asset and vulnerability repository.

IRS personnel stated that for Operating System 2 and Operating System 3, there are multiple technical and resource limitations affecting the compliance scores. The IRS has multiple Plans of Action and Milestones in place to document and track the limitations that exist on the Mainframe Platform Environment. The Mainframe Platform Environment staff tracked and monitored their configuration status and have documented their limitations.

We reviewed the January 23, 2024, IRS Configuration Compliance Tool Dashboard report for the Security Application Environment and found that 371 (80 percent) of the total 466 assets are noncompliant, while the remaining 95 (20 percent) are complaint. A follow-up review of the IRS Configuration Compliance Tool Dashboard report from July 25, 2024, found that 695 (90 percent) of the total 770 assets were noncompliant, while the remaining 75 (10 percent) were compliant. The Security Application Environment staff has no documentation for limitations causing a lack of oversight and remediation of noncompliant assets. The existence of noncompliant configurations increases the risk to the overall security of IRS assets.

Recommendation 6: The Chief Information Officer should resolve configuration compliance settings in accordance with Federal and IRS policies.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will develop a solution to review configuration settings to ensure that GSS and Major Application assets meet Federal and IRS policies.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the IRS effectively assigned information technology assets and addressed security vulnerability and configuration issues on one General Support System and one Major Application. To accomplish this objective, we:

- Assessed the IRS's asset and vulnerability repository by determining whether assets were assigned to temporary or unknown GSSs and if assets are assigned to multiple GSSs or Major Applications.
- Determined if the IRS remediated vulnerabilities timely by assessing vulnerability data and reviewing vulnerability scan reports.
- Evaluated the vulnerability remediation process and procedures for assigning assets to major applications by interviewing Cybersecurity and Enterprise Operations function personnel and reviewing documented policies and procedures.
- Determined the IRS's compliance with Federal and agency configuration requirements by reviewing asset configuration data and configuration compliance reports.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity, Enterprise Operations, and User and Network Services functions located at the New Carrollton Federal Building in Lanham, Maryland, during the period December 2023 through August 2024. 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 Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Kasey Koontz, Director; Khafil-Deen Shonekan, Audit Manager; Jin Lee, Auditor; Nicholas Reyes, Auditor; Laura Christoffersen, Information Technology Specialist; and Lance Welling, Information Technology Specialist.

Data Validation Methodology

We obtained data directly from the asset and vulnerability repository. We completed a data reliability assessment to ensure that the data are sufficiently reliable to use to complete our audit objectives. We compared the data from the January 2024 asset and vulnerability repository to the July 2024 data. We also validated the data reports to ensure that the information was accurate and complete by discussing the results with IRS management and making comparisons with other available data to determine its reasonableness. We determined that the data 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: processes, policies, procedures, and guidelines related to the management of information technology assets, vulnerability resolution, and configuration management. We evaluated these controls by interviewing Information Technology organization personnel and analyzing the IRS's asset, vulnerability, and configuration repositories.

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; 582 assets in the Mainframe Platform Environment and Security Application Environment that had unresolved and overdue vulnerabilities (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We analyzed the July 2024 vulnerability scan reports and found 582 assets (12 assets in the Mainframe Platform Environment and 570 assets in the Security Application Environment) with vulnerabilities that were unresolved and overdue. The existence of unresolved vulnerabilities increases the risk to the overall security of IRS assets. Additionally, IRS vulnerabilities must be prioritized for remediation based on risk, and vulnerabilities with the highest risk must be remediated first.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 185 IP addresses incorrectly identified as having a temporary or unknown GSS (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We compared the population of possible IP addresses for the Mainframe Platform Environment and Security Application Environment to the IP address of the assets identified in the January 2024 temporary and unknown GSS vulnerability reports. We found that the Mainframe Platform Environment had eight IP addresses on the temporary GSS vulnerability report and 115 IP addresses on the unknown vulnerability report totaling 123 IP addresses (8 + 115 = 123). Additionally, the Security Application Environment had three IP addresses on the temporary GSS vulnerability report and 59 IP addresses on the unknown GSS vulnerability report totaling 62 addresses (3 + 59 = 62).

Overall, there was a total of 185 (123 + 62) IP addresses incorrectly identified as having a temporary or unknown GSS. The IRS is in the process of migrating to a new system that will have more robust capabilities and resolve the issue of assets incorrectly assigned to temporary and unknown. Until the new system is functional, assets found in more than one GSS or Major Application calls into question the overall accountability for asset assignment.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 99 IP addresses incorrectly included in the Security Application Environment vulnerability report (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

We compared the population of possible IP addresses for the Security Application Environment to the IP address of the assets identified in the January 2024 vulnerability report and found 99 IP addresses outside the Security Application Environment range defined by the agency. Vulnerability reports with assets assigned outside the prescribed range make it difficult to effectively manage and control the environment using that unique identifier.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 743 assets in the Mainframe Platform Environment or the Security Application Environment that have noncompliant configurations (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

In July 2024, we assessed the Mainframe Platform Environment and the Security Application Environment configuration compliance reports and found 48 noncompliant asset configurations for the Mainframe Platform Environment and 695 noncompliant asset configurations for the Security Application Environment. Overall, a total of 743 (48 + 695 = 743) assets were noncompliant. The existence of noncompliant configurations increases the risk to the overall security of IRS assets.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 12, 2024

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal, Chief Information Officer

Rajiv K. Uppal
Digitally signed by Rajiv K. Uppal
Date: 2024.09.12 11:59:53 -04'00'

SUBJECT: Draft Audit Report – Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement (Audit #2024200004)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. We are aware of the need to further improve how we address vulnerabilities in a timely manner and remain committed to ensuring the security of IRS assets and operating environments.

The IRS continues to focus on improving the critical areas of vulnerability and threat management, asset management and configuration management and monitoring. In some cases, deficiencies identified in this audit report were byproducts of the IRS transitioning to better technology. For example, some overdue and unresolved vulnerabilities were the result of transitioning to a tool with more robust scanning that effectively increased the volume of vulnerabilities identified. The IRS is also in the process of migrating to a new system that will improve asset management capabilities. The IRS agrees with most of the recommendations in the report and has already begun taking steps to address the findings and associated outcome measures. Please reference the attached corrective action plan for details and implementation dates.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Robert Cox, Associate Chief Information Officer for Cybersecurity, at (202) 317-7061.

Attachment

Attachment

Audit# 2024200004, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should timely remediate or mitigate all vulnerabilities in accordance with IRS Policy.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will review vulnerability remediation practices and process that might identify gaps that would prevent the process from working in an effective manner. We will close these gaps and reduce vulnerability percentages by 50%.

IMPLEMENTATION DATE: August 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should ensure that systems are in place to reconcile the temporary and unknown repositories to verify that assets are assigned to an established group.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will take steps to implement zero trust best practices to remove physical assets across the network that's not properly documented across a taxonomy.

IMPLEMENTATION DATE: September 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 3: The Chief Information Officer should ensure that systems are in place to reconcile duplicate accounting of assets in the repository.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will begin collaborating with all authorizing officials on their duplicate assets and their respective FISMA boundaries and reconcile assets with the appropriate business units.

IMPLEMENTATION DATE: November 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Attachment

Audit# 2024200004, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement*

RECOMMENDATION 4: The Chief Information Officer should reconcile assets to reflect the operating environment.

CORRECTIVE ACTION 4: The IRS disagrees with this recommendation. The management of IP addresses is not tied to reconciliation of a specific boundary or technology. IP addresses are assigned in blocks which can be misleading since they are assigned as needed.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): N/A

RECOMMENDATION 5: The Chief Information Officer should evaluate the temporary and unknown repositories to establish ownership of assets.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer will begin collaborating with all authorizing officials on their temporary repositories and reconcile assets with the appropriate business units.

IMPLEMENTATION DATE: November 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 6: The Chief Information Officer should resolve configuration compliance settings in accordance with Federal and IRS policies.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The Chief Information Officer will work to develop a solution to review configuration settings ensuring that GSS and Major Application assets meet Federal and IRS policies.

IMPLEMENTATION DATE: May 15, 2026

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

Appendix IV

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Asset	A major application, general support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.
Change Management	The process responsible for controlling the life cycle of all changes; it enables beneficial changes to be made with minimum disruption to information technology services.
Configuration Management	Establishes proper control over approved project documentation, hardware, and software, and assures changes are authorized, controlled, and tracked.
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
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.
Enterprise Operations	Responsible for providing server and Mainframe computing services for all IRS business entities and taxpayers.
High-Value Assets	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content) making them of particular interest to criminal, politically motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS. The IRM contains the directions employees need to carry out their operational responsibilities.
Internet Protocol Address	Standard protocol for transmission of data from source to destination in packet-switched communications networks and interconnected systems such as networks.
Mainframe	A powerful, multiuser computer capable of simultaneously supporting many hundreds of thousands of users.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Term	Definition
Severity Rating	One of five levels on a ratings scale to describe the risk associated with a vulnerability. The complete scale from lowest risk to highest risk is: Informational, Low, Medium, High, and Critical.
System Boundary	The physical or logical perimeter of a system.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
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

GSS	General Support System
IP	Internet Protocol
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration

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

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

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