

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Vulnerability Scanning and Remediation Processes Need Improvement

December 21, 2021

Report Number: 2022-20-006

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

HIGHLIGHTS: Vulnerability Scanning and Remediation Processes Need Improvement

Final Audit Report issued on December 21, 2021

Report Number 2022-20-006

Why TIGTA Did This Audit

Prior TIGTA audit reports identified issues with scanning all devices, performing credentialed scans, and timely remediating vulnerabilities.

In August 2020, the Cybersecurity function began using a new vulnerability scanning tool which, according to the IRS, scans more network devices more frequently than the previous tool.

This audit was initiated to determine whether the IRS effectively identifies and addresses vulnerabilities on network devices.

Impact on Taxpayers

Security weaknesses within the IRS's management and operations security practices increase the risk to its assets and ability to protect taxpayer information. Failure to resolve or track existing vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

What TIGTA Found

The IRS does not effectively oversee vulnerability remediation across the enterprise. For example, the Patch and Vulnerability Group did not verify or monitor the remediation efforts for all vulnerabilities or consistently track and report vulnerability remediation metrics.

Specifically, [REDACTED]

[REDACTED]. In addition, TIGTA reviewed a judgmental sample of 29 of the top 100 vulnerabilities and found that the IRS did not track the remediation with a documented Plan of Action and Milestones or Risk-Based Decision for 20 (69 percent) of the 29 vulnerabilities reviewed.

There is no formal notification process in place to ensure that the Enterprise Vulnerability Scanning group is made aware of network changes requiring updates to the vulnerability scanning tool. [REDACTED]

The IRS did not have a Plan of Action and Milestones or a Risk-Based Decision in place for 71 (97 percent) of the 73 devices on the vulnerability scanning exception list. However, during our audit work, the IRS took action to add the devices back to the vulnerability scan footprint as of July 2021.

Finally, the IRS did not fully implement privileged access scanning for required devices. [REDACTED]

What TIGTA Recommended

TIGTA made six recommendations that the Chief Information Officer should establish an entity to oversee enterprise-wide vulnerability remediation and ensure that required actions are taken; prioritize the remediation of vulnerabilities that exceeded remediation time frames; document vulnerabilities past remediation time frames as required; develop a process to ensure that network updates that affect vulnerability scanning are communicated; enforce current guidance to periodically review the scanning exception list; and ensure that privileged access scans are completed on required devices.

The IRS agreed with all six recommendations. The IRS plans to establish an entity to oversee enterprise-wide vulnerability remediation; prioritize remediating vulnerabilities exceeding remediation time frames; document vulnerabilities past remediation time frames as required; implement a process to ensure that network updates are communicated properly; enforce current guidance to conduct periodic reviews of the scanning exception list; and ensure that privileged access scans are completed on required devices.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

December 21, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

M. Weir for

FROM:

Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – Vulnerability Scanning and Remediation Processes
Need Improvement (Audit # 202120020)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) effectively identified and addressed vulnerabilities on network devices. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS 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

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 2
<u>Vulnerability Remediation Was Not Effective</u>	Page 2
<u>Recommendations 1 through 3:</u>	Page 5
<u>Network Change Process Was Not Formalized</u>	Page 5
<u>Recommendation 4:</u>	Page 6
<u>Corrective Action Plans Were Not in Place for Scanning Exceptions</u>	Page 6
<u>Recommendation 5:</u>	Page 7
<u>Privileged Access Scanning Was Not Fully Implemented</u>	Page 7
<u>Recommendation 6:</u>	Page 8
<u>Appendices</u>	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 9
<u>Appendix II – Outcome Measures</u>	Page 11
<u>Appendix III – Management’s Response to the Draft Report</u>	Page 12
<u>Appendix IV – Glossary of Terms</u>	Page 16
<u>Appendix V – Abbreviations</u>	Page 18

Background

The Cybersecurity function's mission is to protect taxpayer information and the Internal Revenue Service's (IRS) electronic systems, services, and data from internal and external cyber-related threats. The Cybersecurity function performs its mission by implementing security practices in planning, implementation, management, and operations to preserve the confidentiality, integrity, and availability of IRS data and assets. However, our recent audits identified risks that could adversely affect the Cybersecurity function's ability to fulfill its mission.

From Calendar Years 2017 through 2020, we identified and reported issues with vulnerability¹ scanning and remediation. Specifically, we found that the IRS could not determine whether vulnerability scanning tools were scanning all devices.² In addition, we found that the IRS was not performing credentialed scans and was not timely remediating vulnerabilities.³

Vulnerability scanners are commonly used in organizations to identify known vulnerabilities on hosts and networks and on commonly used operating systems and applications. Scanning tools can proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities. The IRS uses agent-based and remote scanning to perform vulnerability scans. Agent-based scanning eliminates the need for service accounts previously used in remote credentialed scans.

In August 2020, the Cybersecurity function's Enterprise Vulnerability Scanning (EVS) group transitioned to a new enterprise vulnerability scanning tool. To establish a scanning footprint for the tool, the IRS used a combination of the tool's discovery capabilities, data from the previous tool, the User and Network Services (UNS) function's network inventory, and internal reporting from system owners. According to the IRS, the new tool scans more devices more frequently than the previous vulnerability scanning tool. In addition, management officials stated that the IRS made several improvements in vulnerability identification and remediation since the transition, and that the new scanning tool provides continuous network vulnerability monitoring and a comprehensive view of the IRS security posture. For example, one improvement was the integration with an analytics and reporting tool, which provides an enhanced centralized reporting experience where scan results are updated every 24 hours.

System owners from Applications Development, Enterprise Operations, and other IRS functions are responsible for remediating identified vulnerabilities. These functions review vulnerability scan results in the reporting application and work to implement vulnerability remediation. When remediation cannot be implemented, system owners are required to develop a Plan of Action and Milestones (POA&M) for remediation or Authorizing Officials must document the accepted risk to the network through a Risk-Based Decision (RBD). Security weaknesses within

¹ See Appendix IV for a glossary of terms.

² Treasury Inspector General for Tax Administration, Report No. 2017-20-061, *The External Perimeter Was Generally Secure, Though The Security Of Supporting Components Could Be Improved* (Sept. 2017).

³ Treasury Inspector General for Tax Administration, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020).

the IRS's management and operations security practices increase the risk to its assets and ability to protect taxpayer information.

Results of Review

Vulnerability Remediation Was Not Effective

Vulnerability remediation oversight is insufficient

The Internal Revenue Manual (IRM)⁴ states that the Patch and Vulnerability Group (PVG) has responsibility for vulnerability remediation oversight and verification. The original PVG Charter and Concept of Operations, developed in 2018, tasked the PVG to establish a systematic and automated approach to patch and vulnerability management, and create remediation and mitigation policies, processes, and methodology. The PVG also was responsible for tracking and reporting vulnerability and remediation metrics to Cybersecurity function leadership.

The IRS does not effectively oversee vulnerability remediation across the enterprise. Specifically, the PVG only provides remediation oversight for high-priority, enterprise-wide vulnerabilities and remediation efforts for high-visibility programs. The PVG did not verify or monitor the remediation efforts for all vulnerabilities. In addition, the PVG did not consistently track and report vulnerability remediation metrics.

PVG personnel stated that they helped develop requirements for a dashboard within the centralized reporting application so that it could provide business units with the most accurate, timely, and updated vulnerability information. In addition, the PVG incorporated monthly and quarterly trending data into the dashboard for users to measure enterprise, vulnerability, and general support system remediation progress. However, PVG personnel stated that they do not consistently review and report enterprise-wide trending data. Instead, they focus on vulnerability prioritization and remediation for high-visibility programs.

Further, according to the Concept of Operations, the PVG is supposed to collect and track metrics including open and remediated vulnerabilities per severity category as well as the total POA&Ms and their status. The PVG is also supposed to report these metrics to Cybersecurity function leadership for them to assess enterprise patch management. However, the PVG stated that system owners were responsible for using the dashboard to obtain their remediation statuses themselves and report any issues to the Cybersecurity function directly.

The IRS lacked timely vulnerability remediation or necessary POA&Ms or RBDs for prevalent overdue vulnerabilities because it did not actively monitor vulnerability data or remediation efforts at the enterprise level. By not actively monitoring vulnerability remediation efforts, the IRS is exposed to potential threats and vulnerabilities and is at risk of not being in compliance with Federal mandates and legislation.

⁴ IRM 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (Nov. 25, 2020).

During our audit work, the IRS updated the PVG Charter⁵ and Concept of Operations documentation. The revised charter limits PVG oversight responsibilities to data calls, which the PVG explained are high-priority, widely exploited vulnerabilities. The IRS did not reassign responsibilities to oversee vulnerabilities that fall outside this category at an enterprise level.

Vulnerability remediation is not timely

The IRM⁶ states that vulnerabilities shall be prioritized for remediation based on risk (highest to lowest) using the Common Vulnerability Scoring System scores and corresponding severity ratings provided by the scanning tools. Figure 1 shows vulnerability severity ratings and their associated remediation time frames.

Figure 1: 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.

The IRS is not timely remediating vulnerabilities in accordance with the IRM's required time frames. We obtained and analyzed the daily vulnerability scan results for January 29, 2021, and found

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

⁵ IRS, *PVG Charter* (May 24, 2021).

⁶ IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (May 9, 2019).

⁷ The same device may fall in multiple categories, [REDACTED]

[REDACTED]⁸ [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

In June 2021, we met with officials from the Cybersecurity function to discuss their vulnerability remediation efforts. According to management officials, the Cybersecurity function has a team that analyzes critical and high vulnerabilities for critical filing season systems on a weekly basis. In addition, officials stated that they provide reporting to the Information Technology organization's Associate Chief Information Officers every three to six months. We reviewed a June 2021 report which [REDACTED]

The IRS is not remediating vulnerabilities in accordance with IRM requirements because it lacks centralized enterprise-wide oversight to ensure that appropriate actions are taken on systems with vulnerabilities exceeding remediation time frames.

Unremediated vulnerabilities lack corrective action plans

We selected a judgmental sample¹⁰ of 29 (29 percent)¹¹ of the top 100 open vulnerabilities across all severity levels, selecting vulnerabilities with the highest number of devices per vulnerability. The IRS did not track the remediation with a documented POA&M or RBD for 20 (69 percent) of the 29 vulnerabilities reviewed. IRS Standard Operating Procedures¹² states that Federal Information Security Modernization Act legislation mandates that all Federal agencies develop and implement a corrective action plan in a POA&M to identify and document the resolution of information security weaknesses. The IRM¹³ requires system owners to develop POA&Ms for remediation or Authorizing Officials to document the accepted risk to the network through a RBD when remediation cannot be implemented. The IRS is not ensuring that vulnerabilities exceeding remediation timeframes are being tracked as required because it lacks centralized enterprise-wide oversight to provide visibility and tracking of aging vulnerabilities that would require POA&Ms or RBDs. Failure to resolve or track existing vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

⁸ The same device may fall in multiple categories, [REDACTED]

⁹ Due to time and resource constraints, we did not validate the accuracy and reliability of the data.

¹⁰ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

¹¹ Our judgmental sample of [REDACTED]

¹² IRS, *Enterprise FISMA POA&M Standard Operating Procedures* (June 2020).

¹³ IRM 10.8.2, *Information Technology Security Roles and Responsibilities* (Nov. 27, 2019).

The Chief Information Officer should:

Recommendation 1: Establish an entity to oversee enterprise-wide vulnerability remediation to ensure that vulnerabilities are remediated within required time frames, POA&Ms and RBDs are documented as required, and vulnerability remediation metrics are reviewed and reported to appropriate leadership.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will establish an entity to oversee enterprise-wide vulnerability remediation to ensure that vulnerabilities are remediated within required time frames, POA&Ms and RBDs are documented as required, and vulnerability remediation metrics are reviewed and reported to appropriate leadership.

Recommendation 2: Prioritize the remediation of vulnerabilities that exceeded remediation time frames.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will establish prioritization for the remediation of vulnerabilities that exceeded remediation time frames documented within the audit report.

Recommendation 3: Ensure that vulnerabilities that exceeded remediation time frames are documented with POA&Ms or RBDs as required.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will ensure that vulnerabilities that exceeded remediation time frames identified within the report are documented with POA&Ms or RBDs as appropriate.

Network Change Process Was Not Formalized

The IRS does not have a formal process to document how to identify when changes¹⁴ occur in the IRS networks or to coordinate with the EVS group so that changes can be made to the vulnerability scanning tool. We reviewed various reports of active network blocks¹⁵ maintained by the UNS function and compared them to a list of network blocks scanned on April 5, 2021, by the IRS's enterprise vulnerability scanning tool. There were [REDACTED]

[REDACTED]. In June 2020, we presented our analysis to the Cybersecurity and UNS functions. The UNS function determined [REDACTED]

During our audit work, the UNS function stated that there is no formal notification process in place to ensure that the EVS group is made aware of network changes requiring updates to the vulnerability scanning tool because there was no requirement to do so. However, in

¹⁴ A change could be starting or stopping the use of a network block, adding new segments to an existing network block, or consolidating multiple smaller networks into a larger network block.

¹⁵ We are substituting the term network block in place of the technical term Classless Inter-Domain Routing Blocks. Classless Inter-Domain Routing Blocks are groups of Internet Protocol addresses that share the same prefix and contain the same number of bits.

August 2021, the UNS function stated that the EVS group will be providing requirements and collaborating with various UNS groups to develop a process document that will include notification to the EVS group of network block allocation and activation to allow for vulnerability scanning. A target date for completion will be determined after the requirements gathering and analysis is completed.

Failing to have a process that identifies changes to active network blocks requiring vulnerability scanning increases the risk that information technology systems not receiving vulnerability scans could be exploited, potentially exposing taxpayer data and information.

Recommendation 4: The Chief Information Officer should develop a process to ensure that network updates that affect vulnerability scanning are properly communicated.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will implement a process to ensure that network updates are properly communicated related to vulnerability scanning.

Corrective Action Plans Were Not in Place for Scanning Exceptions

The IRS did not have POA&Ms or RBDs in place for devices that were not receiving network vulnerability scans. Specifically, 71 (97 percent) of 73 devices on the May 2021 Vulnerability Scanning Exception List did not have a POA&M or RBD in place for not meeting the vulnerability scanning requirements.

The IRM requires all systems and hosted applications to be scanned for vulnerabilities and to document cybersecurity weaknesses that need corrective action in a POA&M. The EVS group's Standard Operating Procedures¹⁶ states that system owners can request an exception to vulnerability scanning due to performance degradation. It states that the EVS group places devices on a scanning exception list for 30 days while the system owner, assisted by the Cybersecurity function, further analyzes the root cause of the performance degradation. If the issue cannot be rectified within the 30-day time frame, the system owner shall submit a POA&M to resolve it. It also states that, if the scanning exception cannot be remediated, the system owner will submit an RBD to the Authorizing Official for approval.

According to the Standard Operating Procedures, EVS personnel are required to conduct periodic reviews of the exception list. We met with EVS personnel, who stated that the EVS group reviewed the scanning exception list monthly and received progress updates, based on POA&Ms or RBDs, from system owners for when vulnerability scanning could resume. However, these monthly reviews did not identify the 71 devices that required a POA&M. Of the 71 devices without a POA&M, 69 had been on the list for more than 150 days, while the other two did not have dates listed.

When we asked why the 71 devices did not have POA&Ms, EVS personnel stated that they were not aware of whether POA&Ms did or did not exist for those devices because system owners only provided POA&Ms when requested by EVS personnel. EVS personnel also stated that they would request POA&Ms from the system owners of these devices as a condition for remaining on the scanning exception list. Because the EVS group did not effectively implement its

¹⁶ IRS, *Enterprise Vulnerability Scanning Standard Operating Procedures* (Nov. 2020).

Standard Operating Procedures, devices did not receive vulnerability scans and corrective actions were not documented as required.

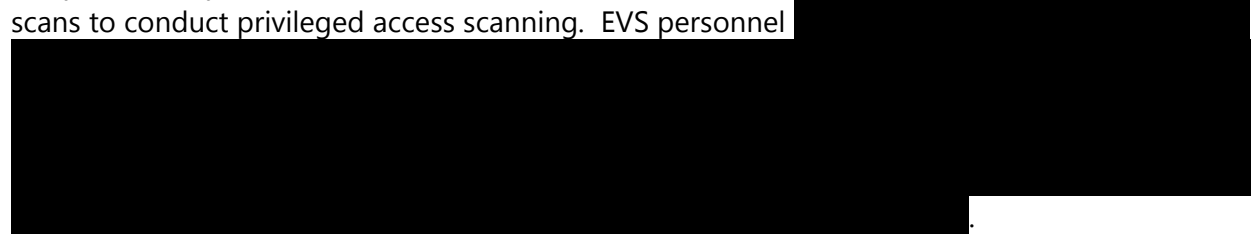
Management Action: During our audit work, the IRS removed the 71 devices without POA&Ms from the scanning exception list. The devices were added back to the vulnerability scanning footprint as of July 2021.

Recommendation 5: The Chief Information Officer should enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking required documentation are added back to the vulnerability scanning footprint as required.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking the required documentation are added back to the vulnerability scanning footprint.

Privileged Access Scanning Was Not Fully Implemented

The IRS did not fully implement privileged access scanning for required devices. According to Cybersecurity function personnel, the EVS uses either scanning agents or remote credentialed scans to conduct privileged access scanning. EVS personnel



The IRM requires the implementation of privileged access authorization for information system components to facilitate more thorough vulnerability scanning. The EVS Standard Operating Procedures states that operating systems are to receive both remote and agent scans daily.¹⁷

EVS personnel stated that the vulnerability scanning tool had scanning agents available for installation on network devices based on their operating systems. EVS personnel explained that when installing an agent inhibited the functionality of the device, the EVS then implemented remote credentialed scans. According to EVS personnel, they reviewed dashboards within the centralized reporting application on a daily basis to ensure that both agent and credentialed scans were successful. However, EVS personnel stated that devices without agents were not receiving credentialed scans for varying reasons including devices being used as temporary or test devices, pending agent installation, and not being provisioned to receive remote credentialed scans. By not fully implementing privileged access scanning, vulnerability assessments are not complete which potentially increases the risk of exposure to taxpayer data and information.

¹⁷ 

Recommendation 6: The Chief Information Officer should ensure that privileged access scans are completed on required devices to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will ensure that privileged access scans are completed on required devices to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS effectively identified and addressed vulnerabilities on network devices. To accomplish our objective, we:

- Reviewed UNS reports of active network blocks and compared them to a list of network blocks scanned by the enterprise vulnerability scanning tool. We also interviewed IRS employees to review and validate our analysis to determine whether the IRS is effectively performing vulnerability scans on its network devices.
- Reviewed vulnerability scan exclusion reports to identify the list of network devices that are excluded from vulnerability scanning and to determine whether POA&Ms or RBDs existed for all devices on the report. We also met with EVS personnel to determine how frequently the exclusion report is updated.
- Reviewed system reports to determine whether network devices that do not have an agent installed received remote credentialed scans.
- Reviewed and analyzed the January 29, 2021, security vulnerability scan report for the enterprise to identify open vulnerabilities that were not remediated timely and closed vulnerabilities that were remediated after required time frames. We also selected a judgmental sample¹ of 29 of the top 100 open vulnerabilities to determine whether vulnerabilities that were not timely remediated had a POA&M or RBD as required. We selected a judgmental sample because we did not plan to project the results to the population.
- Reviewed relevant IRMs, program charters, and the Concept of Operations to determine the responsibilities of the PVG for vulnerability remediation. We also interviewed IRS employees in the PVG to determine if the PVG is actively monitoring vulnerability remediation progress.

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 January through October 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; Andrea Nowell, Lead Auditor; Mike Mohrman, Senior Auditor; and Lance Welling, Information Technology Specialist (Data Analytics).

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the centralized reporting application. We evaluated the data by 1) validating a random sample of data values against source file values, 2) matching imported data sets to raw data counts, and 3) receiving raw data sets from IRS personnel knowledgeable about the data. 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: IRM policies related to vulnerability scanning, remediation, and oversight, and Standard Operating Procedures for establishing POA&Ms and requesting an exception from vulnerability scanning. We evaluated these controls by interviewing Cybersecurity, Applications Development, Enterprise Operations, and UNS function personnel. We also reviewed documentation including policies and procedures related to establishing the vulnerability scan footprint, performance of vulnerability scanning and remediation, and reports of vulnerability scanning results.

Appendix II

Outcome Measures

This appendix presents detailed information on the measurable impacts 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]

(see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

Our data analytics team analyzed the January 29, 2021, [REDACTED]

Type and Value of Outcome Measure:

- Protection of Resources – Potential; [REDACTED]

(see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

We compared various reports of active network blocks to a list of network blocks scanned on April 5, 2021, and [REDACTED]

Appendix III

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Tommy A. Nancy A. Sieger Smith
Chief Information Officer

SUBJECT: Draft Audit Report – Vulnerability Scanning and Remediation Processes Need Improvement (Audit # 202120020) (e-trak #2022-43884)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. The Internal Revenue Service (IRS) is committed to continuously improving cybersecurity by leveraging industry-leading technology that further protects taxpayer data from an evolving and complex threat environment.

Over the last year, the IRS has significantly enhanced the Enterprise Vulnerability Scanning program. Our analysis from June 2021 found that we successfully identified and addressed 97 percent of the critical and high findings for filing season applications, and we have centralized enterprise-wide oversight for the most critical systems that maintain filing season and taxpayer data. For the remaining systems and applications, we have continuous vulnerability monitoring in place that provides a comprehensive and real-time view of the IRS security posture. We also rely on automated patching to manage vulnerability remediation for more than 80,000 workstations which can be challenging due to the complexity of a remote environment and workstations being offline. In fiscal year 2021, the IRS timely addressed more than 1,200 critical vulnerabilities totaling more than 71 million unique updates. We agree with the recommendations and outcome measures in this report and have included a corrective action plan.

The IRS values the continued support, assistance, and guidance provided by your office. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Christopher Pleffner, Director, Cybersecurity Security Risk Management at (240) 613-6169.

Attachment

Attachment

Draft Audit Report – Vulnerability Scanning and Remediation Processes Need Improvements (Audit #202120020)

RECOMMENDATION 1: The Chief Information Officer should establish an entity to oversee enterprise-wide vulnerability remediation to ensure vulnerabilities are remediated within required timeframes, POA&Ms and RBDs are documented as required, and vulnerability remediation metrics are reviewed and reported to appropriate leadership.

CORRECTIVE ACTION #1:

The IRS agrees with this recommendation. IT will establish an entity to oversee enterprise-wide vulnerability remediation to ensure vulnerabilities are remediated within required time frames, POA&Ms and RBDs are documented as required, and vulnerability remediation metrics are reviewed and reported to appropriate leadership.

IMPLEMENTATION DATE: September 15, 2023

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

RECOMMENDATION 2: The Chief Information Officer should prioritize the remediation of vulnerabilities that exceeded remediation time frames.

CORRECTIVE ACTION #2:

The IRS agrees with this recommendation. IT will establish prioritization for the remediation of vulnerabilities that exceeded remediation time frames documented within the audit report.

IMPLEMENTATION DATE: March 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

RECOMMENDATION 3: The Chief Information Officer should ensure that vulnerabilities that exceeded remediation time frames are documented with POA&Ms or RBDs as required.

Attachment

Draft Audit Report – Vulnerability Scanning and Remediation Processes Need Improvements (Audit #202120020)

CORRECTIVE ACTION #3:

The IRS agrees with this recommendation. IT will ensure that vulnerabilities that exceeded remediation time frames identified within the report, are documented with POA&Ms or RBDs as appropriate.

IMPLEMENTATION DATE: March 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

RECOMMENDATION 4: The Chief Information Officer should develop a process to ensure that network updates that affect vulnerability scanning are properly communicated.

CORRECTIVE ACTION #4:

The IRS agrees with this recommendation. IT will implement a process to ensure that network updates are properly communicated related to vulnerability scanning.

IMPLEMENTATION DATE: February 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, User Network & Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

RECOMMENDATION 5: The Chief Information Officer should enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking required documentation are added back to the vulnerability scanning footprint as required.

CORRECTIVE ACTION #5:

The IRS agrees with this recommendation. IT will enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking the required documentation are added back to the vulnerability scanning footprint.

IMPLEMENTATION DATE: March 15, 2022

Attachment

Draft Audit Report – Vulnerability Scanning and Remediation Processes Need Improvements (Audit #202120020)

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress on a monthly basis until completion.

RECOMMENDATION 6: The Chief Information Officer should ensure that privileged access scans are completed on required devices to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

CORRECTIVE ACTION #6:

The IRS agrees with this recommendation. IT will ensure that privileged access scans are completed on required devices to determine the full extent of vulnerabilities affecting the installed operating systems and applications.

IMPLEMENTATION DATE: July 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Agent	A lightweight, low-footprint program installed locally on hosts to supplement traditional network-based scanning or to provide visibility into gaps that are missed by traditional scanning. It collects vulnerability, compliance, and system data, and reports that information back for analysis.
Authorizing Official	The person accountable for the security risks associated with information system operations and with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Common Vulnerability Scoring System	Provides an open framework to communicate the characteristics and impacts of information technology vulnerabilities. It attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
Credentialed Scan	Scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that cannot be seen from the network.
Cyber Hygiene Report	A weekly report by the Cybersecurity function and Infrastructure Security Agency that leverages the Common Vulnerability Scoring System.
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, related to progress and performance.
Data Call	A tool that creates a structured framework for all IRS business units and stakeholders to communicate an emerging vulnerability, threat, risk, or exposure initiated by IRS leadership, the Department of the Treasury, or the Department of Homeland Security.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Federal Information Security Modernization Act of 2014	An amendment to The Federal Information Security Management Act of 2002 that allows for further reform to Federal information security, signed 12 years after the passing of the original law. This bill amends Chapter 35 of Title 44 of the United States Code (Pub. L. No. 113-283). The original statute requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget.

Term	Definition
Internal Revenue Manual	The primary source of instructions to employees related to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Operating System	The master control program that runs a computer, serving as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Plan of Action and Milestones	A document of the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities. The document is prepared for both systems and programs.
Privilege	A right granted to an individual, a program, or a process.
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.
Vulnerability	A weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.

Appendix V

Abbreviations

EVS	Enterprise Vulnerability Scanning
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
POA&M	Plan of Action and Milestones
PVG	Patch and Vulnerability Group
RBD	Risk-Based Decision
UNS	User and Network Services



**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.