TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved

September 20, 2017

Reference Number: 2017-20-061

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.

Redaction Legend:
2 = Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

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.

THE EXTERNAL NETWORK PERIMETER WAS GENERALLY SECURE, THOUGH THE SECURITY OF SUPPORTING COMPONENTS COULD BE IMPROVED

Highlights

Final Report issued on September 20, 2017

Highlights of Reference Number: 2017-20-061 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

As part of its Future State initiative to facilitate voluntary compliance by empowering taxpayers with secure innovative tools and support, the IRS uses numerous public facing information systems on its IRS.gov website to engage taxpayers for tax administration purposes. These systems may process and store Personally Identifiable Information and tax return data for millions of taxpayers. Because this information is considered extremely valuable, the IRS has become a target of cyber criminals and identity thieves. As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the effectiveness of the network perimeter security controls to protect the IRS against external threats and cyberattacks. To assist with this objective, TIGTA hired a contractor to perform penetration testing that simulated an advanced, highly funded attacker attempting to gain access to IRS sensitive systems and information through the Internet. TIGTA also completed audit steps to determine whether the IRS had implemented adequate policies and procedures for maintaining a secure perimeter and correcting reported vulnerabilities in a timely manner.

WHAT TIGTA FOUND

TIGTA's contractor found that the IRS network perimeter, within the scope of its assessment, had applicable security measures against cyberattacks. Other recently performed IRS penetration tests on its network perimeter and web applications have generally found it secure as well.

However, the component inventory for its perimeter environment was inaccurate and incomplete. Various perimeter security system scan reports did not align with the components in the IRS's official enterprise inventory system. Without an accurate inventory, the IRS cannot ensure that it is properly monitoring and maintaining all its perimeter components in a secure manner.

In addition, the IRS was not timely correcting vulnerabilities identified by scans primarily due to the lack of resources. Various perimeter security system scan reports showed several servers had high-level vulnerabilities, some of which continued to be present month after month. TIGTA also identified improvements over vulnerability remediation tracking, metrics, and the need for an escalation process. Known vulnerabilities that are not timely corrected pose an unnecessary risk of exploitation, which may result in compromised systems and loss of taxpayer data.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS Chief Information Officer: 1) ensure that the perimeter inventory is accurate and includes the level of granularity necessary for tracking and reporting; 2) improve processes to ensure that all vulnerability findings are reviewed, analyzed, and appropriately addressed within the required time frames; and 3) ensure that the Security Regulatory Compliance Operations group improves its remediation tracking process.

The IRS agreed with all the recommendations. The IRS plans to enhance and update inventory procedures, improve processes over vulnerability findings, and improve vulnerability remediation tracking and escalation.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 20, 2017

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved (Audit # 201620004)

This report presents the results of our review to evaluate the effectiveness of the network perimeter security controls to protect the Internal Revenue Service (IRS) against external threats and cyberattacks. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix IV.

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

Abbreviations

GSS	General Support System
IP	Internet Protocol
IRS	Internal Revenue Service
KISAM	Knowledge Incident/Problem Service Asset Management
PTCA	Penetration Testing and Code Analysis
SRCO	Security Regulatory Compliance Operations
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) has made many changes in recent years improving tax processing systems, increasing electronic filing and payment options, and expanding services available on IRS.gov for taxpayers and tax professionals. As the needs of taxpayers, the tax community, and the Nation continue to rapidly evolve, the IRS needs to look at the future in a more comprehensive way. Preparing the IRS to adapt to the changing needs of taxpayers is described generally as the IRS Future State initiative. For one of the themes of this initiative, the IRS will facilitate voluntary compliance by empowering taxpayers with secure innovative tools and support.

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS.

The IRS uses numerous public facing information systems on its IRS.gov website to engage taxpayers for tax administration purposes. These systems may process and store Personally Identifiable Information and tax return data for millions of taxpayers. Because this information is considered extremely valuable, the IRS has become a target of cybercriminals and identity thieves. As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS. A strong information security program, including implementation of effective security controls, is needed at the IRS to protect the confidentiality, integrity, and availability of its systems and taxpayer data. The mission of the IRS may be seriously undermined if the systems and data used to meet tax administration responsibilities are not secure from unauthorized access and misuse.

One way to assess the security posture of an organization is by conducting penetration testing. Penetration testing is a security evaluation method in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It involves launching real attacks on real systems and data with tools and techniques commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability. Threats such as organized crime groups and nation states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts.

The National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, provides guidance for penetration testing and states that it is an important tool to help determine the vulnerability of an organization's

network and the level of damage that can occur if a network is compromised. It states that, to simulate an external attack, testers should be provided with no real information about the target environment other than targeted Internet Protocol (IP) addresses or address ranges, and should perform open source research by collecting information on the targets from public web pages or similar sites. After identifying hosts on the network that can be reached from outside, testers should attempt to compromise one of the hosts. If successful, this access may then be used to compromise other hosts that are not generally accessible from outside the network.

To assess the security of the IRS's perimeter network, the Treasury Inspector General for Tax Administration (TIGTA) contracted with Veris Group LLC[1] to perform penetration testing that simulated an advanced, highly funded attacker attempting to gain access to the IRS's sensitive systems and information through the Internet. The contractor assessed the IRS's perimeter systems from an external, black-box perspective; that is, from the perspective of an external hacker that does not have any prior knowledge or information regarding the IRS's systems or its perimeter infrastructure. This testing, as well as additional audit steps performed by TIGTA, assessed how well the IRS was protecting its network perimeter from cyberattacks and other threats.

This review was performed at the Veris Group office in Sterling, Virginia, in November and December 2016, and with information obtained from the IRS Information Technology organization's Cybersecurity and User and Network Services organizations during the period December 2016 through June 2017. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] Veris Group, a provider of cyber risk assessment and technical testing services since 2005, was acquired in December 2016 by Coalfire, a leader in cyber risk management and compliance services.

Results of Review

Penetration Testing Showed That the Internal Revenue Service's Network Perimeter Was Generally Secure

TIGTA's contractor found that the IRS perimeter within the scope of the assessment provided applicable security measures against attacks

TIGTA contracted with Veris Group LLC to perform an external penetration test of the IRS's perimeter infrastructure to test for flaws in configuration, access control management, or other common security issues. This assessment focused specifically on external facing IRS systems, web applications, and supporting components. As agreed to by TIGTA and the IRS's Chief Information Officer prior to the testing, the scope of this assessment was limited to external IP address ranges belonging to the IRS and select IP addresses used by Accenture to operate the IRS.gov website. The scope of this assessment did not include IP addresses registered to the IRS but used by third parties.

The contractor found that the IRS perimeter, within the scope of the assessment, has applicable security measures against attacks. The contractor determined that the IRS platform (within the testable scope) presented a very limited attack surface, and as assessed, sufficiently protected against the most common attack vectors that threaten externally hosted services. The contractor indicated that the IRS's use of strong input filtering and validation on its websites mitigated the possibilities for attacks, and that its web application firewalls ensured that repeated attacks could not successfully be carried out. The IRS's network controls also successfully detected the contractor's assessment activities and blocked access promptly upon perceiving a threat.

During its assessment, the contractor identified two minor issues, which included the presence of an anonymous File Transfer Protocol server and several services exposed externally without a known purpose. The contractor indicated that none of these issues posed a significant security risk for the IRS. The IRS responded that it had accepted the risk of the File Transfer Protocol server as a business requirement to provide taxpayers and organizations with the ability to perform bulk downloads of publicly available content on the IRS.gov website. The IRS indicated that it plans to retire the anonymous File Transfer Protocol capability by October 2017. The IRS also responded that it had completed and approved security documentation for the externally exposed services noted by the contractor.

Other IRS penetration tests also indicated its perimeter is generally secure

Recently completed IRS penetration testing on its perimeter and web applications has generally found the perimeter secure as well. For example, the IRS regularly conducts Qualys vulnerability scans[2] on its externally facing applications. We noted that total confirmed vulnerabilities reported by these scans reduced from 127 in November 2015 to 46 in January 2017, none of which were critical or urgent. IRS policy also requires that compliance verification and vulnerability scans are run at a minimum of monthly on its perimeter components to ensure that each comply with required configuration and security settings.

In addition, in September 2016, the IRS awarded a one-year contract to Synack[3] to provide penetration testing. Synack uses a team of ethical hackers who work from an adversarial perspective to uncover hidden vulnerabilities in IRS perimeter systems. As of January 2017, Synack had identified 17 vulnerabilities related to the IRS perimeter and online applications, including three vulnerabilities rated as a high-level vulnerability by the Common Vulnerability Scoring System.[4] The IRS indicated it had corrected the three high-level and one medium-level vulnerabilities, but had not addressed 13 additional medium-level vulnerabilities.

Further, in October 2016, the Department of Homeland Security National Cybersecurity Assessment and Technical Services team conducted a Risk and Vulnerability Assessment (as mandated by the Office of Management and Budget) on IP addresses associated with two IRS high-value assets and selected internal IP address ranges provided by the IRS. The National Cybersecurity Assessment and Technical Services team also conducts a weekly external vulnerability scan to search for issues on the IRS's external network. The weekly scan revealed an administrative interface which could permit an attack to gain control of the network router, which was deemed a medium-level vulnerability. The IRS indicated it has corrected the vulnerability.

[2] Qualys Web Application Scanning is a commercial off-the-shelf product that provides automated testing of custom web applications to identify vulnerabilities including, but not limited to, cross-site scripting and Structured Query Language injection.
[3] Synack was founded by security experts in 2013 and provides customers a scalable, continuous, hacker-powered intelligence platform that uncovers security vulnerabilities that often remain undetected by traditional penetration testers and scanners.
[4] The Common Vulnerability Scoring System provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. It is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores.

Prior to the Get Transcript online application being redeployed in June 2016, the IRS's Penetration Testing and Code Analysis (PTCA) team,[5] MITRE,[6] and the Department of Homeland Security National Cybersecurity Assessment and Technical Services team each conducted penetration testing on the associated online applications. These tests resulted in a total of one moderate-risk finding and 18 low-risk findings, of which the IRS corrected, placed in corrective action plans, or approved risk-based decisions.

We believe the IRS's current level of testing meets Federal guidelines for maintaining a secure perimeter. However, we found improvements are needed to ensure that the IRS perimeter inventory is accurate and complete, and that the vulnerabilities identified by scans are timely addressed.

The Perimeter Inventory Was Inaccurate and Incomplete

IRS policy[7] requires system owners to develop and document an inventory of information system components that is accurate, includes all components within the authorization boundary of the information system, captures both hardware and software, and is at the level of granularity deemed necessary for tracking and reporting. IRS policy also requires, specifically for high-level impact systems, that automated mechanisms be employed to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. In addition, IRS policy requires the IRS to verify at a minimum of monthly, using compliance verification and vulnerability scanning tools, that all IRS systems comply with required configuration and security settings.

The IRS's perimeter security system, also referred to as General Support System 1 (GSS-1), provides network infrastructure services to IRS personnel and information systems across the Nation, and serves as the IRS Federal Information Security Modernization Act boundary for monitoring and controlling communications with external networks and information systems. The IRS maintains inventory records for its trackable components in its Knowledge Incident/Problem Service Asset Management (KISAM) inventory system,[8] which is its official enterprise inventory system. Each month, GSS-1 staff obtained an inventory update for the GSS-1 components from the KISAM system and placed the list in the GSS-1's file in the

[5] The PTCA is part of the Cybersecurity organization's Security Risk Management organization and is tasked with conducting security assessments of IRS applications and infrastructure, to include penetration testing, vulnerability scanning, and source code reviews. The PTCA team can be contacted by other IRS organizations or system owners to request penetration testing on their systems.
[6] The MITRE Corporation was hired by the IRS to provide independent, expert, and objective advice and guidance on strategic, technical, and program management issues.
[7] Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* pp. 74, 76, 77, and 142 (July 2015).
[8] Trackable components (also called assets) are those that are barcoded for inventory purposes and include laptops, desktop computers, servers, and network devices (such as firewalls, routers, and switches).

Treasury Federal Information Security Modernization Act Information Management System. However, the inventory files from the KISAM system were inaccurate and incomplete.

The IRS accomplishes its scanning requirements of its perimeter components by using various tools, including policy checkers, Tripwire, and Guidelines, Standards, and Procedures scans. We requested the IRS provide us the scans performed on the GSS-1 components for the months of August, September, and October 2016. However, the scans that the IRS provided did not align with the components in the KISAM system inventory lists. To illustrate, we noted the following discrepancies when comparing the scan reports to the relevant inventory list:

- The IRS provided policy checker reports for only 39 of the 282 servers listed in the September 2016 KISAM system inventory and provided reports for 49 servers that were not listed.
- The IRS provided Tripwire reports for only 19 of the 263 servers listed in the January 2017 KISAM system inventory[9] and provided reports for 144 servers that were not listed.
- The IRS provided Guidelines, Standards, and Procedures scan reports for only 112 of the total 190 firewalls, routers, and switches listed in the September 2016 inventory, and provided reports for 41 devices that were not listed. The IRS subsequently indicated that the 41 devices were in the KISAM system inventory, but that data discrepancies in various KISAM system fields needed to be input or corrected.

Based on discrepancies between the GSS-1 inventory lists and the monthly scans provided by the IRS, we could not determine whether all GSS-1 components were being scanned as required. In addition, the GSS-1 inventories listed in its system security plan and its information system contingency plan were inaccurate, inconsistent, and outdated. The IRS indicated that there was a lack of coordination on its part to provide a full response to our request, and that monthly scans were being performed on all components. However, the IRS also indicated that it needed to complete a visual audit of the GSS-1 components to ensure the accuracy of the inventory. As of June 8, 2017, work was still ongoing to complete this effort and to validate the accuracy of key data fields in the KISAM system. The IRS indicated that after completion of correcting the inventory, it would ensure that all GSS-1 components were being scanned.

The KISAM system does not sufficiently use automated means to maintain an up-to-date, complete, and accurate inventory. The KISAM system requires manual updates which can lead to discrepancies. Without an accurate GSS-1 inventory, the IRS cannot ensure that it is properly monitoring and maintaining all its perimeter supporting components in a secure manner.

[9] We compared the Tripwire reports against the January 2017 GSS-1 inventory because the IRS initially only provided Tripwire reports for servers that had high-level vulnerabilities during the months of August through October 2016. At our second request for the Tripwire reports for all GSS-1 servers, the IRS provided reports for the months of December 2016 through February 2017. Therefore, we compared the Tripwire reports against the January 2017 GSS-1 inventory.

Recommendation

Recommendation 1: The Chief Information Officer should ensure that comprehensive and accurate inventories of information system components are maintained, including the GSS-1 inventory, that include the level of granularity necessary for tracking and reporting, and should implement improved procedures for ensuring that the inventory remains accurate and up-to-date.

> ***Management 's Response:*** The IRS agreed with this recommendation. The User and Network Services organization will enhance and update the existing Standard Operating Procedure and continue efforts to ensure that the GSS-1 inventory of information system components is appropriately maintained.

Vulnerabilities Identified by Scans Were Not Timely Corrected

IRS policy[10] requires scans of information systems for vulnerabilities on at least a monthly basis, and remediation of vulnerabilities according to the response times set for the severity level or rank (priority) of the vulnerability. The response time is 30 days for critical and high-level vulnerabilities, 90 days for medium-level vulnerabilities, and 150 days for low-level vulnerabilities.[11]

Although the IRS did not provide all scans for the GSS-1 components listed in its inventory for the three months that we requested (as previously mentioned), the scans that were provided revealed that vulnerabilities were not being remediated within the response times set by IRS policy. We identified instances in which high-level vulnerabilities were not corrected within the 30-day required time frame and medium-level vulnerabilities were not corrected within the 90-day required period. The IRS indicated that, due to resource constraints, it is not addressing repeated medium- or low-level vulnerabilities until it completes its work to address its high-level vulnerabilities. However, the scan reports we reviewed revealed that not all high-level vulnerabilities were being corrected timely, in addition to the medium- and low-level vulnerabilities that also persisted.

- **Policy Checker Reports** – We requested policy checker reports for 88 servers for the months of August, September, and October 2016. The IRS provided us with 87 policy checker reports for August 2016, 11 reports for September 2016, and 48 reports for October 2016. These reports identified high-level vulnerability totals of 145, two, and 30

[10] Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* p. 142 (July 2015), in accordance with National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[11] Internal Revenue Manual 10.8.50, *Information Technology (IT) Security, Servicewide Security Patch Management* (Apr. 2016), in accordance with Treasury Directive Program 85-01, *Treasury Information Technology Security Program* (Nov. 2006) and National Institute of Standards and Technology Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* (July 2013).

in their respective months, and showed that 39 of the 88 servers had one or more high-level vulnerabilities.

The IRS provided policy checker reports for these three months but only for 10 of the 88 servers. These reports identified that one server had a high-level vulnerability that existed all three months. An additional 12 of the 88 servers had a total of 27 high-level vulnerabilities reported in both their August and October 2016 policy checker reports. Although the September scans were not provided for these servers, we believe these vulnerabilities existed for all three months as well. Examples of the repeated high-level vulnerabilities included **********2********** **********2********** . Based on the number of policy checker reports that were not provided, we are concerned that additional repeated high-level vulnerabilities exist that are not being addressed timely.

- **Tripwire Reports** – The IRS provided Tripwire scans for 163 servers for the months of December 2016 through February 2017. Fourteen of the 163 servers had a total of 37 high-level vulnerabilities that existed all three months. Examples of the repeated high-level vulnerabilities related to **********2********** **********2********** **********2********** ***2****. Also, 53 of the 163 servers had 237 medium-level vulnerabilities that existed all three months.

- **Guidelines, Standards, and Procedures Reports** – The IRS provided Guidelines, Standards, and Procedures reports for 153 IP addresses for the months of August, September, and October 2016. Ninety-seven of the 153 IP addresses had a total of 170 high-level vulnerabilities that existed all three months. In addition, the 153 IP addresses had a total of 1,726 medium-level vulnerabilities that existed all three months.

  The IRS implemented automated scanning of its firewall, router, and switches in January 2016, which updates a dashboard daily with compliance data. As of the end of May 2017, the Guidelines, Standards, and Procedures Compliance Dashboard reported that a total of 196 firewalls, routers, and switches residing in the Common Communication Gateway[12] had only a 22 percent compliance rate and a total of 128 high-risk rule violations. The IRS indicated that because network device scanning processes were still maturing, and Guidelines, Standards, and Procedures were being revised, a backlog of vulnerabilities still exist.

Further, a Nessus scan, that was run in December 2016 by TIGTA's contractor on the 48 perimeter hosts that were discovered during the penetration testing, reported a total of

[12] The Common Communication Gateway is what the IRS calls its demilitarized zone which provides Internet connectivity and external data connectivity to Federal, State, and local government agencies and tax partners.

97 medium-level vulnerabilities that included **********2********** **********2**********.

The IRS indicated that difficulties in correcting vulnerabilities were partly due to the existence of legacy devices and limited resources to replace them. Also, due to limited resources, the IRS indicated medium-level vulnerabilities would be worked on by the system administrators as soon as high-level vulnerabilities were corrected.

Vulnerability remediation management needs improvement

To address its vulnerability remediation management, the IRS created the Security Regulatory Compliance Operations (SRCO) group in January 2012. According to the Vulnerability Management Reporting Standard Operating Procedures, the SRCO group is responsible for retrieving the monthly (or weekly) scan results,[13] analyzing the critical and high-level vulnerabilities, developing reports and mitigation recommendations, distributing Vulnerability Analysis Reports to the appropriate stakeholders, and tracking vulnerability remediation. At this time, the Vulnerability Analysis Reports sent to stakeholders only contain critical and high-level vulnerabilities because the IRS indicated it does not have the resources to address the medium-level vulnerabilities until it addresses the high-level vulnerabilities. The intention of the SRCO group in providing the reports to the appropriate stakeholders is to ensure that the findings on the noncompliant devices are remediated during the time frames specified by IRS policy. However, as we have illustrated with the examples of repeated high-level vulnerabilities, the process is not working as intended.

To be more effective, we believe SRCO processes should track the actual age of the vulnerabilities, create monthly metrics to monitor remediation status, and implement an escalation process that provides management visibility.

- **Track actual age of vulnerabilities** – As high-level vulnerabilities continue to be reported in the monthly scans, the SRCO group continues to include them in the monthly Vulnerability Analysis Reports to stakeholders. However, the report does not capture when the vulnerability was first seen on the component. Tripwire has the capability to record the actual age of the vulnerability in a field labeled "first seen date." However, in the Tripwire scans we reviewed, these dates were never more than two months old for the vulnerabilities that were repeated every month from December 2016 to February 2017. Rather, in each month the "first seen date" field was reset to be no more than two months old. The IRS indicated that the reset of the date was a technological limitation caused by the IRS's processes to archive the monthly Tripwire data. However, using this Tripwire

[13] The IRS PTCA team and the User and Network Services organization are responsible for executing the monthly (or weekly) scans to identify vulnerabilities and ensuring that the scan results are made available to the SRCO group.

feature, or another means to capture the "first seen date," would aid the IRS in tracking the actual age of vulnerabilities for more effective remediation tracking.

- **Create monthly metrics** – The Standard Operating Procedures state that the SRCO group should create monthly metrics for critical and high-level vulnerabilities. Cybersecurity officials indicated that the Vulnerability Analysis Reports were serving this purpose. While the reports serve as some notice and reminder to stakeholders that high-level vulnerabilities continue to exist, these reports do not constitute monthly metrics to be used by management to assess the IRS's progress in vulnerability remediation. Metrics that include summary information, such as the number of vulnerabilities still open or closed from month to month, would be more useful for monitoring progress.
- **Implement escalation process** – The Standard Operating Procedures further state that if a timely response to vulnerability management inquiries is not received, the SRCO group should escalate the issue to the Director, Cybersecurity Operations. However, the SRCO group indicated that the Standard Operating Procedures did not sufficiently include implementation of an escalation process that would provide management visibility, which the SRCO group indicated was needed to increase its effectiveness for tracking remediation of high vulnerabilities.

Failure to eliminate high-level vulnerability findings from the vulnerability scans compromises the security posture of the system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation. Failure to eliminate medium- and low-level vulnerabilities, and allowing the number of them to go unchecked, can collectively raise the risk of system compromise and loss of taxpayer data.

Recommendations

The Chief Information Officer should:

Recommendation 2: Improve processes to ensure that all vulnerability findings are reviewed, analyzed, and appropriately addressed within the required time frames.

> ***Management's Response:*** The IRS agreed with the recommendation. The Cybersecurity organization will establish a new group to review and analyze the existing processes, and identify recommended changes that will address findings associated with the GSS and within the designated time frames.

Recommendation 3: Ensure that the SRCO group improves its remediation tracking processes to include tracking the age of the vulnerability, creating monthly metrics to be used by management to assess the IRS's progress in vulnerability remediation, and implementing an escalation process that provides management visibility.

Management's Response: The IRS agreed with the recommendation. The Cybersecurity organization will improve the remediation of age vulnerability findings associated with the GSS. The IRS is developing a process to track and perform monthly metrics, which will include an escalation process, and to assess vulnerability status and remediation.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the effectiveness of the network perimeter security controls to protect the IRS against external threats and cyberattacks. To accomplish our objective, we:

I. Determined whether written policies and procedures for ensuring that the network perimeter is secure were in accordance with Federal guidelines and have been effectively implemented.

A. Obtained and reviewed relevant documents to determine whether the IRS's written policies and procedures for ensuring that network perimeter security were in accordance with Federal guidelines, to include applicable National Institute of Standards and Technology standards, Office of Management and Budget standards, Department of the Treasury policy, and IRS policy.

B. Interviewed the IRS's PTCA team to determine its role in IRS perimeter penetration testing.

C. Obtained and reviewed all recent IRS perimeter penetration test reports produced by the PTCA team, Department of Homeland Security, or IRS contractors, and identified the security weaknesses from these efforts as well as the related corrective actions proposed to remediate the security vulnerabilities.

D. Contracted with the Veris Group to conduct a penetration test of the IRS's external network. We obtained and reviewed the Veris Group penetration test report and identified the reported security weaknesses and related corrective actions proposed to remediate them.

II. Determined whether IRS network perimeter security weaknesses were timely corrected.

A. For the weaknesses identified by the PTCA, the Veris Group, and the other entities identified in Step I, evaluated the IRS's corrective actions and determined whether they were timely.

B. Reviewed the IRS Perimeter Security System (GSS-1) security documents, *e.g.*, System Security Plan, annual testing results, and security assessment reports, and determined whether reported weaknesses were corrected timely.

C. Determined whether the IRS maintains secure configurations on its perimeter components.

1. Reviewed monthly scan reports, *e.g.*, policy checkers, Tripwire, for all perimeter components (servers, firewalls, routers, and switches) for the months of August,

September, and October 2016 to identify vulnerabilities and determine whether they were resolved timely.

III. Determined whether the IRS's information security detection and response capabilities were effective at mitigating the impacts of attacks from advanced actors, including whether the IRS detected the contractor's assessment activities and took proper actions once the perceived attack was detected.

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: Internal Revenue Manual Sections 10.8.1 and 10.8.50, and other IRS controls and procedures related to protecting the IRS network perimeter and correcting vulnerabilities in a timely manner. We evaluated these controls by interviewing IRS management and staff; reviewing relevant National Institute of Standards and Technology, Office of Management and Budget, Department of the Treasury, and IRS documentation; and reviewing relevant supporting documentation.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Linda Cieslak, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner - Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Enterprise Technology Implementation
Director, Network Engineering
Director, Office of Audit Coordination

Appendix IV

Management's Response to the Draft Report

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

AUG 18 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: for S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved (Audit # 201620004) (e-trak #2017-94732)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate the audit team's acknowledgement that the Internal Revenue Service (IRS) network perimeter had applicable security measures to fend off cyber-attacks. We are pleased the audit team found the IRS platform presented a very limited attack surface, and sufficiently protected against common attack vectors that threaten externally hosted services.

The IRS continues to improve the protection of its perimeter systems and web applications through penetration testing, regularly conducting scans, and mitigating all level vulnerabilities. We are currently expanding the Vulnerability Management function to oversee all components of our process, which includes steps to review, analyze, track, prioritize, escalate and remediate vulnerabilities timely.

The attached is our detailed planned corrective actions to implement the audit report's recommendations for process improvement. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment

Attachment

Draft Audit Report The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved (Audit # 201620004)

RECOMMENDATION #1: The Chief Information Officer should ensure that comprehensive and accurate inventories of information system components are maintained, including the GSS-1 inventory, that include the level of granularity necessary for tracking and reporting, and should implement improved procedures for ensuring the inventory remains accurate and up-to-date.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The User and Network Services organization will enhance and update the existing Standard Operating Procedure, and continue efforts to ensure the GSS-1 inventory of information system components are appropriately maintained.

IMPLEMENTATION DATE: September 15, 2018

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 monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should improve processes to ensure that all vulnerability findings are reviewed, analyzed, and appropriately addressed within the required time frames.

CORRECTIVE ACTION #2: IRS agrees with the recommendation. The Cybersecurity organization will establish a new group, to review and analyze the existing processes and identify recommended changes that will address findings associated with the General Support System and within the designated timeframes.

IMPLEMENTATION DATE: June 15, 2018

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 monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Chief Information Officer should ensure that the SRCO group improves its remediation tracking processes to include tracking the age of the vulnerability, creating monthly metrics to be used by management to assess the IRS's progress in vulnerability remediation, and implementing an escalation process that provides management visibility.

Attachment

Draft Audit Report The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved (Audit # 201620004)

CORRECTIVE ACTION #3: IRS agrees with the recommendation. The Cybersecurity organization will improve the remediation of age vulnerability findings associated with the General Support System. We are developing a process to track and perform monthly metrics, which will include an escalation process, to assess vulnerability status and remediation.

IMPLEMENTATION DATE: December 15, 2018

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 monitor them on a monthly basis until completion.