TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners

October 24, 2016

Reference Number: 2017-20-004

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 = Risk Circumvention of Agency Regulation or Statute

.

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.

IMPROVEMENTS ARE NEEDED TO ENSURE THE PROTECTION OF DATA TRANSFERS TO EXTERNAL PARTNERS

Highlights

Final Report issued on October 24, 2016

Highlights of Reference Number: 2017-20-004 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The IRS shares data with various outside entities including Federal, State, and local agencies; financial institutions; and contractors for tax administration purposes. The data may include sensitive information, such as Personally Identifiable Information and taxpayer information. IRS and Federal guidelines require that sensitive data be protected during transmission to prevent unauthorized access or disclosure.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS is properly protecting the data it transmits to external entities through secure file transfer technology. TIGTA determined whether the IRS was maintaining encryption controls and other security configurations in accordance with the National Institute of Standards and Technology.

WHAT TIGTA FOUND

The IRS uses three methods to transfer data to external partners: 1) a commercial off-the-shelf product for transfers over the Internet, 2) a commercial off-the-shelf product for direct mainframe-to-mainframe data transfers, and 3) drop boxes to allow the IRS and its external partners to place and retrieve data transfers. In reviewing all three of these external file transfer methods, TIGTA found the IRS did not ensure that encryption requirements are being enforced and ensure that nonsecure protocols are not being used in order to fully protect information during transmission. These protocols include File Transfer Protocol and Telnet, which are known insecure transfer protocols.

The IRS also did not remediate high-risk vulnerabilities or install security patches on file transfer servers in a timely manner. For example, TIGTA found 61 servers with high-risk vulnerabilities, 10 servers with outdated versions of Windows and UNIX operating systems still in operation, and 32 servers missing 18 unique security patches, of which four were deemed as critical.

Lastly, the IRS did not ensure that corrective action plans for correcting security control weaknesses, including some of the weaknesses previously mentioned, met IRS standards. This reduced the assurance that the weaknesses would be corrected timely.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer enforce IRS policy to encrypt all data transmissions from end-to-end using Federally compliant encryption, or if external partners cannot use Federally compliant encryption, ensure that risk-based decisions have been properly approved and data transmissions have been properly authorized; ensure that file transfer components are properly configured, patching is timely, and outdated operating systems are replaced; centralize and consolidate the IRS's external transfer environment to the extent possible**,** using a managed file transfer solution that supports end-to-end Federally compliant encryption to maximize security and efficiency; and ensure that remediation plans are effective for correcting weaknesses in a timely manner.

The IRS agreed to ensure that data transmissions are properly authorized and remediation plans for correcting weaknesses are effective. The IRS partially agreed regarding end-to-end encryption enforcement, proper configurations, patching, and operating systems, indicating that it already had processes in place. The IRS disagreed that it could further consolidate its external file transfer environment but would reconsider as partner agreements are revalidated. TIGTA believes the IRS should proactively work with partners to upgrade to end-to-end encryption solutions rather than waiting because the data transmitted are highly sensitive.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 24, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners (Audit # 201620006)

This report presents the results of our review of whether the Internal Revenue Service is properly protecting the data it transmits to external entities through secure file transfer technology. This audit was included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

- Encryption Was Not Fully Implemented for All Data Transfers ..... Page 3
  - Recommendation 1: ..... Page 5
  - Recommendation 2: ..... Page 6
- File Transfer Servers Were Not Always Securely Configured, and Reported Vulnerabilities Were Not Timely Remediated ..... Page 6
  - Recommendation 3 through 5: ..... Page 10
- Plans of Action and Milestones for Correcting Weaknesses Need Improvement ..... Page 11
  - Recommendation 6: ..... Page 13

Appendices

- Appendix I – Detailed Objective, Scope, and Methodology ..... Page 14
- Appendix II – Major Contributors to This Report ..... Page 16
- Appendix III – Report Distribution List ..... Page 17
- Appendix IV – Management's Response to the Draft Report ..... Page 18

Abbreviations

DMZ	Demilitarized Zone
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTP	File Transfer Protocol
IPsec	Internet Protocol Security
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement National Institute
NIST	of Standards and Technology Plan of Action and
POA&M	Milestones
UPC	UNIX Policy Checker
WPC	Windows Policy Checker

Background

The Internal Revenue Service (IRS) shares data with various outside entities including Federal, State, and local agencies; financial institutions; and contractors for tax administration purposes. The data may include sensitive information, such as Personally Identifiable Information, and taxpayer financial and tax information. IRS and Federal guidelines require that sensitive data be protected during transmission to prevent unauthorized access or disclosure.

IRS and Federal guidelines require that sensitive data be protected during transmission to prevent unauthorized access or disclosure.

Current IRS solutions for external file transfers

The IRS currently uses three methods to transfer data to external partners.

- The IRS uses a commercial off-the-shelf managed file transfer product for many of its outbound and inbound data transfers. As of June 2016, the IRS had created 348 accounts for data-sharing purposes using this managed file transfer product. The managed file transfer servers reside both within the IRS's internal network and within its demilitarized zone (DMZ),[1] which the IRS refers to as its Common Communication Gateway.[2] Data are held, stored, received, or streamed to external partners through the managed file transfer servers in the DMZ.
- The IRS uses a second commercial off-the-shelf product for transferring data directly from its mainframe to external partners' mainframes. The IRS exchanges data through this direct connection method with 10 other Federal agencies. Data are exchanged through Internet Protocol Security (IPsec)[3] tunnels that exist between the agencies' data centers. The network path between the two mainframes includes the IRS's intranet and its DMZ.
- The IRS uses drop boxes to exchange data. Drop boxes are servers located within the IRS DMZ that use various other software products and transfer protocols, and are

[1] In computer security, a demilitarized zone, or DMZ, is a network segment inserted as a "neutral zone" between an organization's private network and the Internet. Its purpose is to enforce the internal network's information security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
[2] The Common Community Gateway, which is the IRS's DMZ, serves as concentration points for all IRS external data connectivity to Federal and local government agencies and tax partners. In addition, it also provides Internet connectivity for the IRS.
[3] A suite of protocols for securing Internet Protocol communications at the network layer by authenticating and/or encrypting each Internet Protocol packet in a data stream.

accessed by external partners to retrieve files placed into them by the IRS, or for the IRS to retrieve files placed into them by external partners.

In order to protect the data being shared, IRS policy requires that minimum baseline security configurations be maintained for its information systems and system components, including the communications and connectivity-related aspects of its systems, in accordance with the National Institute of Standards and Technology (NIST) standards. In addition, IRS policy requires that data be encrypted during transmission and that the flow of information between interconnected systems be authorized. IRS policy also prohibits the use of nonsecure network protocols such as File Transfer Protocol (FTP),[4] Trivial FTP,[5] and Telnet.[6]

Secure firewall configurations are needed to protect file transfers

IRS firewalls[7] are managed by the IRS's User and Network Services organization. Any changes to firewall configurations must be approved by the IRS's Computer Security Incident Response Center based on a Firewall Change Request form. Firewalls play an important role in ensuring that inbound and outbound data are being protected and are responsible for protecting IRS infrastructure, systems, and applications from threats originating from the IRS intranet or the Internet. The firewalls inspect traffic on a particular network segment and determine the validity of a packet before allowing it to pass into a successive network zone. For data exchanges with external partners, IRS firewall administrators must set up and maintain firewall configurations to allow external trading communications into the DMZ and/or the IRS internal network, thereby raising the risk profile for potential security breaches via the trading partner tunnels.

This review was performed with information obtained from the IRS Information Technology Cybersecurity; Enterprise Operations; User and Network Services; and Privacy, Governmental Liaison, and Disclosure offices primarily located at the New Carrollton Federal Building in Lanham, Maryland, during the period November 2015 through July 2016. 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 objectives. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[4] The FTP is a standard Internet protocol for transmitting files between computers on the Internet. It was originally defined in 1971 without much concern for security.
[5] Trivial FTP is an Internet software utility for transferring files that is simpler to use than FTP but less capable. It is used where user authentication and directory visibility are not required.
[6] Telnet is a user command and protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely.
[7] A firewall device controls the flow of network traffic and limits access between networks and/or systems based on specific security policy.

Results of Review

Our review of the three external file transfer methods in use at the IRS indicated that these methods have the capacity to meet Federal Standards for encryption and other compliance requirements. However, the IRS had not always implemented or maintained required security controls within its file transfer components to ensure the protection of the data being transmitted. Further, the IRS did not remediate reported vulnerabilities in a timely manner. In addition, the IRS may be inefficiently utilizing its limited resources by having to support multiple platforms for transferring files.

Encryption Was Not Fully Implemented for All Data Transfers

IRS policy requires IRS information systems to implement encryption mechanisms to prevent unauthorized disclosure and changes to information during transmission. It prohibits the use of nonsecure network protocols, such as FTP, Trivial FTP, and Telnet because these types of data transmissions are not encrypted. It also requires the IRS to review information systems at least annually to identify unnecessary and/or nonsecure functions, ports, protocols, and/or services, and to disable those deemed unnecessary and/or nonsecure.

The IRS did not ensure that encryption requirements are being enforced and that nonsecure protocols, including FTP and Telnet, are not being used in order to fully protect information during transmission. The IRS stated it cannot fully enforce encryption requirements or disallow use of the nonsecure protocols because not all of its external partners that trade data with the IRS can comply with encryption requirements. The IRS indicated that all traffic, including traffic using the FTP and Telnet protocols, is sent through encrypted IPsec tunnels from the IRS external boundary to the external partner's external boundary. However, not all data transfers are encrypted as they are transmitted through the DMZ prior to entering the IPsec tunnel. This results in the data traversing the DMZ in clear text that could be intercepted.

Within the managed file transfer environment, the IRS had not enabled a setting called Federal Information Processing Standard (FIPS) Transfer Mode, which requires the sender and recipient to use only FIPS 140-2 encryption[8] to ensure that the entire transfer is secure. Enabling the setting would cause transfers to fail if one of the servers (sender or recipient) did not have encryption capabilities. Therefore, the IRS had not enabled the setting in order to accommodate

[8] FIPS 140-2, *Security Requirements for Cryptographic Modules*, is the standard issued by the NIST that specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

external partners that do not meet Federal encryption standards. The IRS was unable to determine during our audit how many external partners do not comply with Federal standard encryption and therefore need to be accommodated. The IRS indicated a change request was prepared in July 2016 to modify ciphers within the managed file transfer solution to ensure compliance with Federal encryption standards.

Similarly, the IRS has not enforced encryption requirements or disallowed nonsecure transfer protocols for all transfers using the direct transfer or drop box solutions. Although the IRS is using IPsec tunnels to encrypt the information as it travels on the Internet between the IRS and its external partners, the data are transmitted across both parties' DMZ in clear text. We reviewed 24 drop box servers located in the DMZ and found 15 servers that were running the FTP, of which nine servers were also running Telnet.

We also reviewed 88 firewall rulesets that the IRS identified were involved in external file transfers. Of the 88 rulesets, 29 rulesets allowed FTP, Telnet, and/or Trivial FTP. Specifically, there were 24 allowances of FTP, 15 of Telnet, and five of Trivial FTP, as some rulesets allowed one or more of these protocols. The types of sensitive data being exchanged through these firewalls include taxpayer data, bank data, financial and corporate data, law enforcement data, examination results, and data traveling from IRS international sites (including China, Hong Kong, and Mexico City) to U.S. Customs.

The IRS stated that there have been ongoing efforts over the past two years to validate firewall rules in order to remove unnecessary legacy rules and ensure that traffic is properly flowing through configured rulesets. We requested the IRS review the 29 firewall rulesets that allowed nonsecure traffic through its firewalls and to determine whether an interconnection security agreement (ISA)[9] was in place to authorize and accept the risk of allowing this traffic. The IRS found that many of the rules allowing the nonsecure protocols may be outdated, but that it needed to observe the network traffic to determine whether nonsecure protocols were currently being used. If not, the IRS indicated it would remove the nonsecure protocols from the rulesets. The IRS's review resulted in the deletion, or scheduled deletion, of 13 of the 29 rulesets when it discovered that they were no longer being used.

The IRS stated that all of the firewall rules allowing FTP, Telnet, and Trivial FTP were covered by four ISAs, and one additional ISA that was in process. We reviewed the four approved ISAs to determine whether use of the nonsecure protocols had been authorized. Only one of the four ISAs specified that a nonsecure protocol was in use and was signed by the IRS and the external partner. The other ISAs did not specify use of nonsecure protocols and, therefore, we found no assurance that the nonsecure protocols allowed on the associated firewalls were authorized or even needed. The IRS has not ensured that the ISAs or other approval or authorization

[9] IRS policy requires that connections between IRS information systems and other information systems must be authorized through the ISAs to ensure that all equipment connected to an IRS system or network meets the minimum security requirements defined by applicable Federal information technology security guidance and requirements.

documents associated with these data exchanges are in place to justify or accept the risk of the use of nonsecure protocols. Further, in regards to the ISA awaiting approval, the IRS implemented firewall rulesets allowing nonsecure protocols before the connection was authorized.

In a previous Treasury Inspector General for Tax Administration audit report,[10] the IRS agreed to identify and document external interconnections in a centralized inventory and ensure that all appropriate ISAs (or other approval agreements) were in place before interconnections were allowed to be established and activated. The IRS set the corrective action date to complete these actions as of September 15, 2016.

Until the IRS has better information on its data transfer environment and its partners that require data transfers without encryption, it cannot make a proper determination on whether to accept the risk of continuing to allow the nonsecure protocols, or to enforce its policy to encrypt data transmissions and insist its partners do so as well.

Transmitting unencrypted information puts information at risk of unauthorized disclosure. The data that are transmitted across both parties' DMZ in clear text could lead to unauthorized disclosure in the event the file transfer server is compromised or there is employee malfeasance.

Recommendations

The Chief Information Officer should:

Recommendation 1: Enforce IRS policy to encrypt all data transmissions from end to end using Federally compliant encryption and prohibit nonsecure protocols. In instances when external partners cannot use Federally compliant encryption, ensure that risk-based decisions have been properly approved and data transmissions and transfer protocols have been properly authorized in an ISA.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS responded that all data transmissions are encrypted while in transit over the Internet, but due to external partner technological incompatibilities, there may be instances in which nonsecure protocols are implemented that prevent end-to-end encryption. The IRS will review its current ISAs to ensure that, when nonsecure protocols are in use, they are documented in the appropriate ISA and the risk has been formally documented and accepted.
>
> ***Office of Audit Comment:*** The IRS's partial agreement actually aligns with our recommendation. While we believe the IRS should not allow nonsecure protocols that

[10] Treasury Inspector General for Tax Administration, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* p. 11 (Sept. 2015).

prevent end-to-end encryption, the IRS agreed that it will properly document instances when this occurs as well as its risk acceptance.

Recommendation 2: Continue to work on reviewing the firewall rulesets to remove those that are no longer needed and ensure that only transmissions approved in a current ISA are allowed through the firewalls.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will continue to review its external file transfer firewall rulesets, remove those that are no longer needed, and ensure that only transmissions approved in a current ISA are allowed through the firewalls.

File Transfer Servers Were Not Always Securely Configured, and Reported Vulnerabilities Were Not Timely Remediated

The IRS is not remediating high-risk vulnerabilities or installing security patches on file transfer servers located in the DMZ in a timely manner. The Internal Revenue Manual (IRM) establishes baseline configurations for information systems and system components, including communications and connectivity-related aspects of systems, in accordance with NIST standards. It requires automated mechanisms be employed to centrally manage, apply, and verify configuration settings for information system components. In addition, IRS policy requires that information systems and applications be scanned for improper configurations, software flaws, and other vulnerabilities at least on a monthly basis. The IRM requires the IRS to analyze vulnerability scan reports and to remediate legitimate vulnerabilities in accordance with the response times that align with the severity level of the vulnerability.

The IRS uses automated compliance tools to scan for improper configurations, vulnerabilities, and software flaws. The Windows Policy Checker (WPC), UNIX Policy Checker (UPC), and Mainframe Policy Checker are scans that validate whether configuration settings meet IRS standards. In addition, the IRS uses a Tripwire product, which is an automated scanning solution that monitors for known vulnerabilities.

High-risk vulnerabilities were not timely remediated, and outdated servers are still being operated

We reviewed all available WPC and UPC reports contained in the IRS's database for November 2015, December 2015, and January 2016 for 70 servers (38 Windows servers and 32 UNIX servers) involved in external file transfers that we identified through IRS system documentation. Policy checker reports and Tripwire reports were not available for all three months for every server. The IRS indicated that some of the missing reports were related to these servers being located in the DMZ, requiring manual action to complete scanning and remediation processes.

All 97 WPC reports from 34 servers that we reviewed reported high-risk vulnerabilities. In addition, 43 of 69 UPC reports that we reviewed reported high-risk vulnerabilities. These 43 reports came from 27 UNIX servers. The high-risk vulnerabilities included:

- **********2********** (97 of 97 WPC reports).
- **********2********** (30 of 97 WPC reports).
- **********2********** (26 of 69 UPC reports).
- **********2********** (18 of 69 UPC reports).

We also reviewed Tripwire vulnerability scans that the IRS provided for 55 of the servers we reviewed. Of the total 1,387 vulnerabilities reported, 3 percent (40 of 1,387) were rated high on six servers, 12 percent (173 of 1,387) were rated medium on 28 servers, and 85 percent (1,174 of 1,387) were rated low on 55 servers. The high-risk vulnerabilities included vulnerabilities **********2**********. These vulnerabilities were listed in the Common Vulnerabilities and Exposures[11] database as being identified in Calendar Years 2009 through 2013. The IRS did not indicate why these vulnerabilities had not yet been resolved.

The WPC reports and the Tripwire scans showed a total of six *****2*****servers, which are no longer supported by the vendor.[12] The UPC includes a test for outdated operating systems, but scores it as no risk. The UPCs reported four ***2*** servers that are also no longer fully supported.

The IRS stated it established an enterprise-level Infrastructure Currency team several years ago to address outdated software and hardware. Additionally, the IRS stated it has an extended maintenance contract **********2********** operating system to mitigate security concerns during the upgrade period.

Failure to properly configure system components in accordance with IRM and NIST requirements compromises the security posture of the system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation, all of which compromise the integrity, confidentiality, and availability of the system. Moreover, running outdated and unsupported software increases security exposure, as the vendor will not be supplying any security patches to the unsupported software.

[11] A dictionary of common names for publicly known information system vulnerabilities.
[12] According to Microsoft, Windows 2003 server's end of life occurred in July 2015.

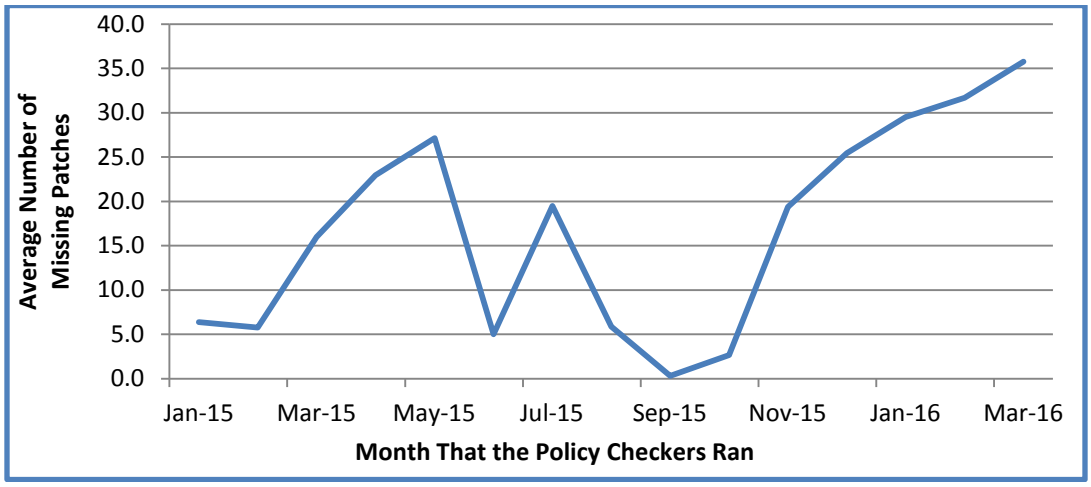
Scans revealed that missing software patches increased month after month

Patch management refers to the process by which an organization installs patches, which are fixes or updates to computer programs, operating systems, or applications. From a security perspective, patch management is an important element in mitigating the security risks associated with known vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a security patch or workaround to mitigate the vulnerability. Any significant delays in finding or fixing software with critical vulnerabilities provide ample opportunity for persistent attackers to break through, gain control over the vulnerable machines, and get access to the sensitive data contained on the computer, destroy information on the computer, or use the computer as a launching point for additional attacks to other computers on the network. For that reason, the IRS mandates that patches need to be installed within certain time frames based on the severity of the vulnerability associated with the patch. This ranges from 30 calendar days for critical vulnerabilities to 150 calendar days for low-risk vulnerabilities.

Our review of the monthly WPC scan reports revealed numerous missing patches. We performed an extended missing patch analysis on the Windows servers in our review from January 2015 through March 2016 based on the Microsoft Baseline Security Analyzer's missing patch list section of the WPC reports and found that server patching was not being done on a regular basis, with an increasing number of unpatched systems throughout most of the year. The number of missing patches ranged from zero in September 2015 up to 47 patches missing in March 2016. Our analysis revealed 32 servers that were missing a total of 120 Microsoft system patches (18 unique patches) that were older than October 2015 and had not been installed by March 2016. Microsoft rated 22 percent of these patches as critical (four of 18), 33 percent (six of 18) as important or moderate, and 6 percent (one of 18) as low. Microsoft did not rate the remaining 39 percent (seven of 18) of the patches.

Figure 1 shows that patching was started between May and July 2015 and was completed in September 2015, with minimal patching being performed throughout the rest of the year. The sharp decline in June 2015 was because the IRS was able to provide only June WPC reports for two servers.

Figure 1: Average Number of Missing Patches From WPC Reports



Source: IRS monthly WPC reports.

During our review, the IRS corrected a number of the high-risk vulnerabilities on these servers that we brought to its attention. The IRS stated that, because these servers are located within the DMZ and not on the main IRS network, patching and configuration management require manual action. That is, system administrators must apply required patches or correct configuration settings on these servers manually, rather than, for example, relying on the IRS's enterprise patch management tools to automatically deploy the patches. The manual action may have contributed to the low compliance levels. The IRS stated that it is creating process improvements to ensure that configuration changes and patches are completed on all servers within the established time frames. By not installing patches in a timely manner, the IRS increases the risk that known vulnerabilities in its systems may be exploited.

Use of a comprehensive managed file transfer solution would maximize security and efficiency

Generally, industry standards prescribe that, if possible, the use of one managed file transfer solution is desirable because it provides a centralized mechanism to govern all enterprise file transfers, offers the most cost and administrative efficiencies, and helps ensure compliance with regulatory mandates and internal security policies. Supporting multiple transfer platforms requires more hardware and software as well as labor resources having subject matter expertise for each of the platform's architectures and technologies. In addition, maintaining outdated file transfer technologies that no longer meet Federal standards poses significant security risks.

The IRS indicated that it maintains a minimum number of external file transfer solutions required to support interfacing with partners, government entities, and other stakeholders and cannot be limited to a single solution. The IRS also indicated it is working towards further minimizing and simplifying its file transfer environment. Implementing a comprehensive managed file transfer solution that consolidates and standardizes external transfers onto a centrally managed platform

and supports end-to-end Federally compliant encryption would maximize security and efficiency. Converting the drop box users to the managed file transfer solution would reduce the number of technologies that the IRS uses and the risk of outdated drop box servers in the DMZ not being securely maintained.

Recommendations

The Chief Information Officer should:

Recommendation 3: Ensure that configuration settings are configured in accordance with IRM requirements and outdated operating systems are replaced.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS responded that it currently has processes in place to ensure that configuration settings are configured in accordance with IRM requirements and to ensure that operating systems are updated as required. Upgrades for the infrastructure supporting the enterprise file transfer capability are targeted to be completed in January 2017.
>
> ***Office of Audit Comment:*** Based on our findings of high-risk vulnerabilities that were not corrected timely and outdated operating systems in use within the DMZ, we believe the processes in place are not fully effective. The IRS needs to ensure that its processes for ensuring proper configurations and for updating operating systems are effectively implemented and make improvements where these controls have broken down.

Recommendation 4: Ensure that patches are applied to file transfer components, including those located in the DMZ, within established time frames.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS responded that it has a process in place to timely implement patches to its information technology infrastructure, including patches to the file transfer components located in the DMZ. The IRS will verify that patching for file transfer components have been applied.
>
> ***Office of Audit Comment:*** Based on our finding of unpatched file transfer components in the DMZ, we believe the process in place is not fully effective. The IRS needs to ensure that its process for timely applying patches is effectively implemented and make improvements where the control has broken down.

Recommendation 5: Centralize and consolidate the IRS's external transfer environment to the extent possible using a managed file transfer solution that supports end-to-end Federally compliant encryption to maximize security and efficiency.

> ***Management's Response:*** The IRS disagreed with this recommendation. The IRS responded that its external transfer environment is already consolidated to the extent

possible based on its mission needs and the statutory and regulatory requirements of its partners. Nonetheless, the IRS will continue to look for ways to migrate external transfers to more centralized approaches as partner agreements are revalidated.

> ***Office of Audit Comment:*** Based on the IRS's statutory and regulatory requirements to protect sensitive and taxpayer data, we believe the IRS should proactively determine which transfers involve nonsecure protocols and/or outdated equipment. The IRS should work with those partners to upgrade to a solution that supports end-to-end Federally compliant encryption rather than wait for the expiration of the current partner agreement because the data transmitted are highly sensitive.

Plans of Action and Milestones for Correcting Weaknesses Need Improvement

The IRS conducts annual testing of system security controls in accordance with the Federal Information Security Modernization Act (FISMA) of 2014[13] requirements. The security control weaknesses previously discussed were among those identified during the IRS's annual testing of system controls on three IRS general support systems that utilize external file transfers solutions, including:

- Encryption controls were not fully implemented.
- Use of nonsecure protocols and/or ports was not restricted.
- Connections were not reviewed, updated, and authorized from the information system to other information systems outside of the authorization boundary through the use of the ISAs.

In general, we found weaknesses in controls important to ensuring the security of file transmissions, including access controls, configuration management, identification and authentication controls, and system interconnection controls.

FISMA legislation mandates that all Federal agencies develop and implement a corrective action plan, known as the Plan of Action and Milestones (POA&M), to identify and document the resolution of information security weaknesses and periodically report progress to the Office of Management and Budget and Congress. The POA&M serves as an authoritative management tool to address and resolve security-related weaknesses within individual IRS information technology programs and information systems. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates. The purpose of the POA&M process is to assist executive and senior leadership in identifying,

[13] Pub. L. No. 113-283. The FISMA defines a framework for managing information security that must be followed for all information systems operated by or on behalf of Federal agencies.

assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and information systems.

The IRS's POA&M Standard Operating Procedures state that a primary cornerstone to developing a sound information security program is the timely identification and resolution of information security weaknesses. The Standard Operating Procedures also state that each new weakness must have a milestone to represent each action required to achieve overall mitigation, as well as an associated due date for each milestone. The milestone steps must include specific actions that need to be taken, coordination that might be needed, obtaining and allocating resources, testing the corrections to ensure that they effectively resolve or mitigate the weakness, and updating documentation to reflect any changes.

We reviewed the POA&Ms prepared for the identified security control weaknesses within the general support systems that use the IRS's external file transfer solutions. While the IRS had prepared the POA&Ms for the identified control weaknesses, it did not ensure that all the POA&Ms met the IRS's standards for including specific actions that would need to be taken to resolve the weakness. Specifically, 25 of the 63 POA&Ms we reviewed did not meet IRS POA&M standards due to the following reasons:

- Milestone actions were not clearly defined or detailed to ensure effective resolution of the weakness (22). The scheduled completion date for eight of these 22 had passed, with the weaknesses remaining uncorrected.
- The POA&M did not address the weakness (3).

In addition, three of the 63 POA&Ms had been closed without sufficient evidence to show the weakness had been corrected.

The IRS indicated that not meeting the scheduled completion dates was not due to the lack of detailed milestones, but was more likely due to conflicts with higher priorities, issues encountered with funding, limited skilled resources, or changes in mitigation strategies that affect the team's ability to meet the initial target completion dates. Also, in those instances, new target completion dates are negotiated and agreed to by the FISMA security team and the operational teams. However, the IRS agreed that there may be instances in which the POA&Ms we reviewed would have been improved with more robust milestone details, as well as determining the root cause of the weakness. Therefore, the IRS will evaluate its current internal processes for reviewing and ensuring compliance with the Enterprise POA&M Standard Operating Procedures to determine if additional validation steps are needed to ensure that the POA&Ms meet IRS policy.

The lack of sufficient processes to ensure that the POA&Ms meet IRS standards reduces assurance that corrective actions will be achieved in a timely manner.

Recommendation

The Chief Information Officer should:

Recommendation 6: Ensure that the POA&Ms are prepared in accordance with IRS policy, including clearly defined milestone steps and identification of resource needs, such that the POA&M is effective for correcting the weakness in a timely manner.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS responded that it has increased its oversight of POA&M development to ensure that they are prepared in accordance with IRS policy.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS is properly protecting the data it transmits to external entities through secure file transfer technology. To accomplish our objective, we:

I. Determined whether external file transfer technologies in use at the IRS meet Federal standards.

   A. Determined whether IRS policies and procedures for external file transfers meet Federal requirements.

   B. Identified file transfer technology currently in use at the IRS for external file transfers and determined whether each has the capability to meet Federal standards.

   C. Determined the monitoring activities the IRS performs to ensure that systems remain in compliance with requirements for secure external file transfers.

   D. Reviewed IRS security documents for the secure file transfer applications (such as the System Security Plan, annual testing results, and security assessment reports) and evaluated any reported weaknesses.

II. Determined whether the IRS has implemented sufficient controls to ensure the security of all external file transfers.

   A. Determined whether firewall rules are implemented appropriately.

   B. Evaluated monthly configuration and vulnerabilities scan reports to determine whether file transfer components were properly configured and patched timely. We evaluated the reliability of the data and concluded that the reports were sufficiently reliable to identify the configuration weaknesses and missing patches associated with the file transfer components. To perform the data reliability and validation, we compared the results of the scans over a period of three months and interviewed IRS managers who were knowledgeable about the report data and scanning processes. The data were used to identify configuration weaknesses and missing patches in file transfer components.

III. Evaluated the effectiveness of the IRS's plan to identify, procure, and implement a managed file solution which addresses current weaknesses and fully complies with secure file transfer requirements.

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 Section 10.8.1[1] and other IRS controls and procedures related to ensuring the security of external file transfers. We evaluated these controls by interviewing IRS management and staff, reviewing relevant NIST and IRS documentation, and reviewing relevant supporting documentation.

[1] IRM Section 10.8.1, *Information Technology Security, Policy and Guidance* (July 8, 2015).

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Lead Auditor
Larry Reimer, Senior Auditor
Esther Wilson, Senior Auditor
Tom Martin, Auditor

Appendix III

Report Distribution List

Commissioner
Officer of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
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

CHIEF INFORMATION OFFICER

SEP 22 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – Controls Over External File Transfers

Thank you for the opportunity to review your draft audit report and provide our comments related to IRS controls over external file transfers. The IRS is fully committed to ensuring that sensitive data is protected during transmission and to preventing unauthorized access or disclosure. We appreciate your acknowledgement that the file transfer methods in use at the IRS are appropriate in terms of their capacity to meet Federal standards for encryption and other compliance requirements.

We appreciate that you acknowledge IRS processes related to configuration management, patch management and other technical controls. We continue to have multiple process improvements underway at the IRS to further ensure the appropriate controls are in place and enforced. Your report specifically, highlights IRS' continual efforts to validate and verify firewall rulesets to ensure authorized transmissions. We have implemented an effective process for the review of firewall rulesets, and we believe the recommendations in the audit serve to validate the importance of the process that is now in place.

We are pleased to say that we are already addressing the recommendations in this report through ongoing process improvement efforts at the IRS. We have already identified outdated operating systems and assessed the associated risk and established an enterprise-level team working on infrastructure currency to manage operating system upgrades. We have developed a strategy to implement enterprise patch management and are making progress in that area. Cybersecurity has also increased oversight in development of Plans of Action and Milestones to improve quality and ensure they are prepared in accordance with IRS policy.

We are committed to continuously improving our information technology systems and processes. We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (240) 613-9373, or have a member of your staff contact Joe Sanchez at (240) 613-4334.

Attachment

Attachment

Draft Audit Report – Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners (Audit # 201620006)

RECOMMENDATION #1:
The Chief Information Officer should enforce IRS policy to encrypt all data transmissions from end to end using Federally-compliant encryption and prohibit non-secure protocols. In instances when external partners cannot use Federally-compliant encryption, ensure that risk-based decisions have been properly approved and data transmissions and transfer protocols have been properly authorized in an ISA.

CORRECTIVE ACTION #1:
IRS partially agrees with this recommendation. 100% of data transmissions are encrypted while in transit over the internet. Due to external partner technological incompatibilities there may be instances where non-secure protocols are implemented that prevent 'end-to-end' encryption, yet these protocols are encapsulated in encrypted VPN tunnels when traversing the internet. IRS will review its current ISAs and when non-secure protocols are required to connect end-to-end, IRS will ensure they are documented within the appropriate ISA and any risk is formally documented and accepted.

IMPLEMENTATION DATE: August 15, 2017

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 #2: Continue to work on reviewing the firewall rulesets to remove those that are no longer needed and ensure that only transmissions approved in a current ISA are allowed through the firewalls.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. IT User and Network Services and Cybersecurity will continue to review the external file transfer firewall rulesets and remove those that are no longer needed. We will ensure that only transmissions, approved in a current ISA, are allowed through the firewalls.

IMPLEMENTATION DATE: January 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User and Network Services

Attachment

Draft Audit Report – Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners (Audit # 201620006)

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: Ensure that configuration settings are configured in accordance with IRM requirements, and outdated operating systems are replaced.

CORRECTIVE ACTION #3:
The IRS partially agrees with this recommendation. IRS currently has processes in place to ensure that configuration settings are configured in accordance with IRM requirements. Configuration settings are documented, reviewed and updated routinely. We will adhere to this process to ensure that configuration settings are configured in accordance with IRM requirements. With respect to outdated operating systems, we also have a process in place to ensure that operating systems are routinely updated as required, contingent on the availability of funding. In this regard, IRS is currently upgrading older Windows servers as part of the Enterprise Windows Upgrade Project and migrating Unix systems to supported Unix platforms. Upgrades for infrastructure supporting the enterprise file transfer capability are targeted to be completed in January 2017.
RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

IMPLEMENTATION DATE: January 15, 2017.

RECOMMENDATION #4: Ensure that patches are applied to file transfer components, including those located in the DMZ, within established time frames.

CORRECTIVE ACTION #4: The IRS partially agrees with this recommendation. The IRS has an enterprise-wide process in place to continuously and timely implement patches to the IT infrastructure. The IRS will follow this process to ensure that patches are applied to file transfer components, including those located in the DMZ, within established time frames. The IRS will verify that patching for file transfer components have been applied.

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

IMPLEMENTATION DATE: January 15, 2017

RECOMMENDATION #5: Centralize and consolidate the IRS's external transfer environment to the extent possible using a managed file transfer solution that supports end to end Federally compliant encryption to maximize security and efficiency.

Attachment

Draft Audit Report – Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners (Audit # 201620006)

CORRECTIVE ACTION #5: The IRS disagrees with this recommendation. The IRS's external transfer environment is already consolidated to the extent possible based on the mission needs of the agency and statutory and regulatory requirements for its partners. Nonetheless, we will continue our standard practice to look for ways to migrate external transfers to more centralized approaches as partner agreements are revalidated.

IMPLEMENTATION DATE: N/A

RECOMMENDATION #6:
The Chief Information Officer should ensure that the POA&Ms are prepared in accordance with IRS policy, including clearly defined milestone steps and identification of resource needs, such that the POA&M is effective for correcting the weakness in a timely manner.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. IRS Cybersecurity has increased its oversight of development of Plans of Action and Milestones to ensure they are prepared in accordance with IRS Policy.

IMPLEMENTATION DATE: September 15, 2017

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.