TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network

August 26, 2008

Reference Number: 2008-20-159

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.

Phone Number | 202-622-6500
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 26, 2008

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network (Audit # 200720015)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) is adequately controlling and securing its web servers. The audit focused on the security over internal web servers on the IRS network. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan and was part of the Information Systems Programs business unit's statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

A web server is a computer that contains the software necessary for a web site to operate. At the time of our review, 1,811 internal web servers on the IRS network had not been approved to connect to the network, and 2,093 internal web servers connected to the network had at least 1 high-, 1 medium-, or 1 low-risk security vulnerability. These unauthorized and insecure web servers placed both the computers and the entire IRS network at risk of unauthorized accesses to taxpayer and personally identifiable information.

Synopsis

The IRS requires that business units register all internal web sites and web servers with the Web Services Division in the Modernization and Information Technology Services organization. We obtained a September 2007 network scan from the IRS Computer Security Incident Response Center that identified 2,093 potential web servers connected to the IRS network. We compared the scan results to the web registration database and identified 1,811 web servers that

were not in the web registration database. These 1,811 web servers were not authorized to connect to the IRS network. We recognize that some of these unauthorized web servers could be legitimate web servers supporting IRS operations. For example, the Enterprise Operations organization was able to show that 661 (36 percent) of the 1,811 web servers had a legitimate business purpose.

The risk exists that the remaining 1,150 unauthorized web servers are being used for non-business purposes. Due to resource constraints, we conducted only limited tests to identify non-business web servers and found none. We did identify situations in which some unauthorized web servers were inadvertently running web services.

We attribute the existence of unauthorized web servers to 1) web server owners not registering their servers with the web registration program, and 2) responsibility for the web registration program remaining unassigned since September 2006. Lack of ownership over the web registration program adversely affected the maintenance and inventory of the web registration database. According to IRS procedures, if a web server is not registered, it might be blocked from delivering information to the network. Because no office had responsibility for the web registration program, this requirement was not enforced, and web servers were allowed to be connected without proper authorization and accountability.

Web servers can pose a security risk to the IRS network. To evaluate compliance with security guidance, we analyzed the September 2007 Computer Security Incident Response Center vulnerability scan, which identified 2,093 authorized and unauthorized web servers with at least 1 high-, 1 medium-, or 1 low-risk security vulnerability. The scan report contained 540 web servers with at least 1 of 160 high-risk vulnerabilities. Unauthorized servers pose a greater risk because the IRS has no way to ensure that they will be continually configured in accordance with security standards and patched[1] when new vulnerabilities are identified. Malicious hackers or disgruntled employees could exploit the vulnerabilities on these web servers to manipulate data on the server or use the servers as a launching point to attack other computers on the network.

In addition to security vulnerabilities, the IRS was using 33 different web server software packages. We believe that using as few products as possible would limit security risks, such as monitoring for security vulnerabilities, and control costs for licensing fees, training, and maintenance.

Recommendations

We recommended that the Chief Information Officer establish official ownership and assign responsibilities for the web registration program, enforce IRS procedures to block unauthorized

[1] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

web servers from providing data over the IRS network, and require an annual scan of web servers and comparison to the web registration database to identify unauthorized web servers. Unauthorized web servers should be immediately disconnected from the IRS network, and inappropriate web sites should be referred to the Treasury Inspector General for Tax Administration Office of Investigations. In addition, web server owners should be required to revalidate the need for the servers annually and immediately notify the Chief Information Officer upon decommission of any web server. The Chief Information Officer should also require quarterly network scans of web servers to measure compliance with security requirements and limit the number of approved web software packages used in the non-modernized environment.

Response

The Chief Information Officer agreed with our recommendations. The Associate Chief Information Officer, Enterprise Operations, was designated as the responsible official for the web registration program and database. The IRS will identify unauthorized web servers and create policies and procedures to prohibit them from providing data over the IRS network. Also, the Computer Security Incident Response Center will perform recurring discoveries of enterprise assets and provide an annual report to the web registration business owner to reconcile discovered assets with those currently registered. Unauthorized web servers will be disconnected, and web sites with inappropriate content will be referred to the Treasury Inspector General for Tax Administration Office of Investigations. In addition, the Computer Security Incident Response Center will perform quarterly security assessment scans to measure compliance with security requirements, and business owners and system administrators will eliminate the vulnerabilities. Lastly, the IRS will investigate the web software packages in use and work with the Office of Enterprise Architecture to create a list of approved software. 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. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services

Background

A web server is a computer that contains the software necessary for a web site to operate. Web sites provide an organization with the means to contact stakeholders, customers, and employees for sharing information, communicating with others, and conducting business. The potential for information sharing is enormous because the Internet is made up of more than 1 billion users and more than 165 million web sites. The Internet is based on the premise of open accessibility.

Using the principles of the Internet, organizations can create internal web sites to share information with employees and allow them to process work. Internal web sites are less expensive to implement than a private network, which is based on proprietary protocols, and are easily accessible by employees. Similar to public web sites, connecting to internal web sites and taking advantage of their benefits also present security risks. These risks include the unauthorized alteration of web site content, disruption of employee access to the web sites and computer operations, and unauthorized access to web server data as well as data on the network to which the web servers are connected.

Internal web sites are generally protected from outsiders by an organization's firewall[1] computers. This protection could give an organization a false sense of security. During the Black Hat Security Conference[2] in August 2007, two leading security professionals demonstrated that advancements in security research will allow hackers to exploit flaws in web browsers and employees' use of web browsers to infiltrate and attack internal web servers with greater ease. They further stated that organizations are unintentionally leaving the door of their information technology operations unlocked by failing to adequately protect their internal web servers. They concluded that organizations should begin defending their internal web servers in the same manner as they safeguard their external web sites.

In September 2007, the Internal Revenue Service (IRS) issued a comprehensive security policy on web servers and web software to better identify security controls and requirements for web servers. The policy established minimum security controls to safeguard both internal and external web servers.

This review focused on internal web servers, and any use of the term "web servers" in this report refers to internal web servers unless otherwise noted. The review was performed at the IRS field

[1] A firewall is a computer with hardware and software that is designed to restrict access to and from an organization's internal network resources.
[2] Black Hat is a computer security conference held throughout the world to discuss computer security issues and events as well as train and inform individuals about security threats that might be present on their computer networks. Black Hat generally consists of computer hackers, security experts, government officials, and network administrators.

offices in Dallas, Texas, and Oakland, California, and at the National Headquarters in New Carrollton, Maryland, in the Office of the Chief Information Officer during the period September 2007 through May 2008. 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.

Results of Review

Unauthorized Web Servers on the Network Pose Significant Risks to Data Protection and Employee Productivity

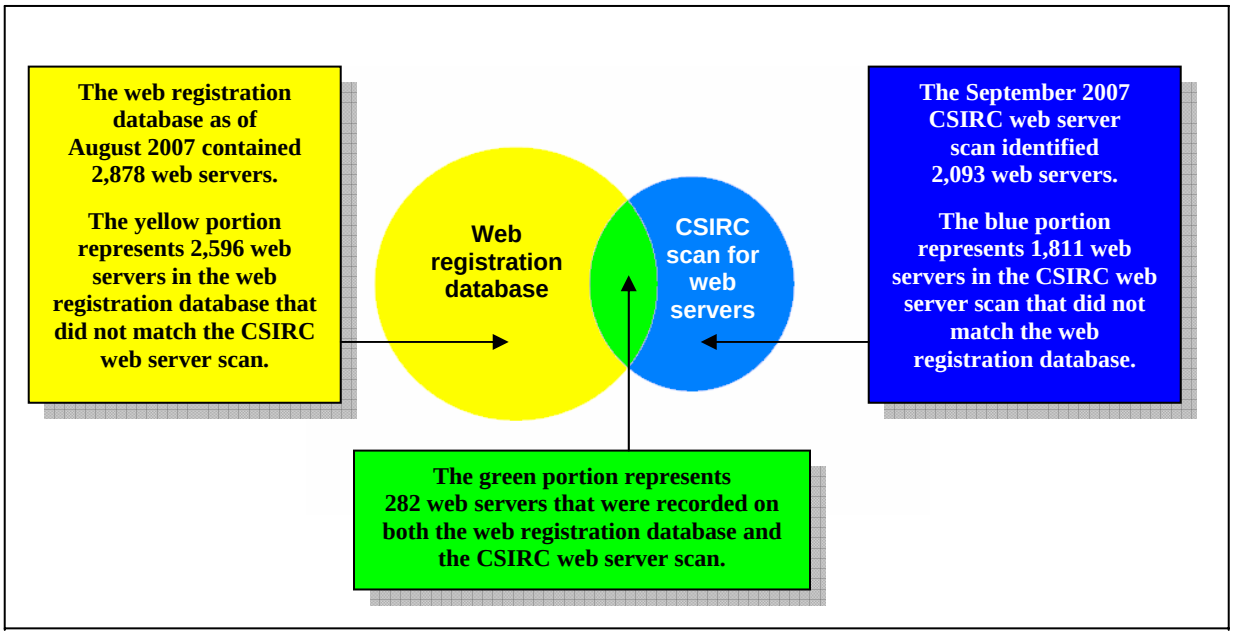
The IRS requires that business units register all internal web sites and servers with the Web Services Division in the Modernization and Information Technology Services (MITS) organization. The registration process–which was effective on April 1, 2006–ensures that a site and server are a known entity on the network, an executive-level sponsor has approved the web server for internal use, and a system administrator and webmaster have been designated to ensure that the server's configurations and content are maintained and updated when necessary. This requirement is the starting point for ensuring that information residing on the IRS network is properly protected and inventoried and data are not compromised.

To support the registration process, the IRS established a database that contains information on all registered web sites and web servers. The information captured includes executive sponsorship, web administrator, content manager, web site name, web site purpose, specific machine name, operating system, and web software. As of August 2007, the IRS web registration database contained 2,878 active web servers.

We obtained a network scan completed in September 2007 by the IRS Computer Security Incident Response Center (CSIRC) to identify all possible web servers actually connected to the IRS network. The scan identified 2,093 potential web servers[3] that were connected to the IRS network. We compared the CSIRC scan results to the web registration database to determine how many web servers on the network had been registered as required. Figure 1 presents the results of the comparison.

[3] Due to the nature of network scans, we did not have absolute assurance that the 2,093 web servers are truly web servers. A network scan generally uses an automated program that attempts to access devices on the network and identify certain characteristics based on a set of criteria. This CSIRC network scan was set to identify characteristics typical for web servers. The possibility exists that other devices could have been identified as web servers, such as multi-functional devices. However, we are confident that most, if not all, of the devices are web servers because the September 2007 scan was refined from an earlier scan by eliminating over 7,400 peripheral devices, such as printers, routers, and switches, and lesser known web server software packages.

Figure 1: Comparison of Web Registration Database Data and CSIRC Web Server Scan



Source: Treasury Inspector General for Tax Administration match of the web registration database, as of August 2007, to the September 2007 CSIRC web server scan.

Our comparison of the web registration database to the CSIRC web server scan found that only 282 web servers were recorded in both data sources, shown as the green portion in Figure 1. We identified 2,596 web servers in the registration database that were not found by the CSIRC scan, shown as the yellow portion in Figure 1. It is likely that many of these web servers were external web servers, no longer in existence, inaccurately recorded on the web registration database, or changed since being registered but not updated on the web registration database.

Of greater concern are the 1,811 web servers identified by the CSIRC scan that were not included in the web registration database, shown as the blue portion in Figure 1. These 1,811 web servers represent those that have not been authorized, yet are connected to the IRS network. However, the unauthorized web servers could be legitimate servers supporting IRS operations. For example, during our review, the Enterprise Operations organization[4] within the MITS was able to demonstrate that 661 (36 percent) of the 1,811 web servers had legitimate business purposes.

Due to time constraints, we conducted only limited tests to determine whether the remaining 1,150 (1,811 – 661) unauthorized web servers were being used for non-business purposes and

[4] The Enterprise Operations organization provides efficient, cost-effective, secure and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.

found none. We did find some that were operating unintentionally as web servers. An unintentional web server might exist when a system administrator inadvertently misconfigures a computer to perform as a web server or is unaware that web server capabilities are installed by default.[5] During our review, we were able to identify whether web servers were laptop and desktop computers[6] based on the computer naming convention. In the population of laptop and desktop computers, we identified the location of 54 unauthorized web servers. We judgmentally selected 19 of these 54 computers at 3 IRS offices and confirmed that they were valid computers on the network but were unintentionally running web services. We advised local system administrators of this situation, and they took actions to disable the web server capability of the computers. Because the remaining 35 laptop and desktop computers were dispersed throughout the country, we were unable to physically verify whether these computers were legitimate web servers.[7] We referred the remaining computers to the CSIRC for further review to determine whether these computers are legitimate computers and authorized web servers.

When we started planning this audit in June 2007, officials from the MITS organization were unable to tell us which office had ownership of the web registration program. As previously discussed, the existing procedures for the web registration process cited the Web Services Division as the responsible office. However, discussions with MITS organization personnel, including a former Web Services Division employee, indicated that the Web Services Division was disbanded in September 2006 and its program areas were dispersed to other MITS organization offices.

The MITS organization did not transfer ownership of the web registration program when the Web Services Division was disbanded in September 2006. Of greater concern, during the course of our audit–when the MITS organization recognized the lack of program ownership–it still had not decided which of its offices should have responsibility for the program. While MITS organization officials did inform us that the web registration program will be taken over by the Enterprise Networks organization,[8] as of April 2008 we were unable to obtain supporting documentation that this transfer was approved and in effect. We believe that lack of ownership

[5] The following is an illustration of an unintentional web server: Internet Information Services 5.0 was installed on Microsoft 2000 Server by default when the operating system was loaded onto server hardware. As such, any Windows 2000 Server built that uses default settings, be it a file server, print server, or domain controller, would have the Internet Information Services 5.0 services installed, running, and listening for calls on the networks. Microsoft addressed this concern by disabling the default installation of Internet Information Services 6.0 on its Windows Server 2003.

[6] While there is no definitive rule that web sites must operate on servers, generally web servers should be computers designated as servers rather than employee workstations. We believe that laptop and desktop computers assigned to individual employees might be more indicative of unintentional web servers.

[7] Among the 35 laptop and desktop computers were 21 computers that supported a Wage and Investment Division customer service program in different IRS field offices. While we were unable to physically verify these computers, we were able to connect with them and validate their purposes.

[8] The Enterprise Networks organization serves to positively satisfy IRS business units' requirements for all forms of electronic communications in the most efficient and effective manner.

over the web registration program adversely affected the maintenance and inventory of the web registration database. According to IRS procedures, unregistered web servers might be blocked from delivering information to the network. Because no office had been given responsibility for the web registration program since September 2006, this requirement was not enforced, and web server owners were allowed to connect their web servers to the IRS network without proper authorization and accountability.

Other organizations under the Chief Information Officer had acknowledged that the web registration database was inaccurate. In August 2007, the Applications Development organization[9] within the MITS reviewed a random sample of 45 computer helpdesk tickets relating to internal web sites and found that 8 of the 45 sites were not registered on the web registration database.

Recommendations

The Chief Information Officer should:

Recommendation 1: Establish official ownership of the web registration program and assign responsibility for the web registration process and the web registration database. Policies and procedures should be updated to reflect the change of ownership.

> ***Management's Response:*** The Chief Information Officer agreed with this recommendation. The Associate Chief Information Officer, Enterprise Operations, was designated as the official for the web registration program and web registration database. Policies and procedures will be updated to reflect the change of ownership.

Recommendation 2: Enforce IRS procedures to block unauthorized web servers from providing data over the IRS network. We recognize that some web servers used for legitimate business purposes might be temporarily blocked during this effort. In these instances, web server owners will have to quickly obtain formal authorization and be reconnected to the network. We believe that blocking the unauthorized web servers is the most effective and efficient approach to obtaining an accurate inventory of authorized web servers.

> ***Management's Response:*** The Chief Information Officer agreed with this recommendation. The IRS will take steps to identify unauthorized web servers and will create a policy and procedure to prohibit them from providing data over the IRS network. The IRS will also establish a process to accommodate legitimate web servers affected by this recommendation.

Recommendation 3: Require an annual scan of web servers and compare the scan results to the web registration database. Unauthorized web servers should be immediately disconnected

[9] The Application Development organization serves as the focal point for the IRS to define, design, build, test, deliver, and maintain integrated information applications systems for developmental and production environments.

from the IRS network architecture, and any web site identified with inappropriate content should be referred to the Treasury Inspector General for Tax Administration Office of Investigations. In addition, owners of registered web servers should be required to revalidate the need for the web servers annually and immediately notify the Chief Information Officer when web servers are decommissioned.

> ***Management's Response:*** The Chief Information Officer agreed with this recommendation. The CSIRC will provide an annual report to the web registration database business owner to reconcile the assets. The IRS will compare the annual scans run by the CSIRC to the web server database and disconnect unauthorized web servers. Web sites identified with inappropriate content will be referred to Treasury Inspector General for Tax Administration Office of Investigations. The IRS will also develop a process to ensure that registered web server owners revalidate the need for the web servers annually and provide notification when web servers are decommissioned.

Security Weaknesses Were Prevalent on All Web Servers Connected to the Network

Lack of program ownership and an inaccurate inventory can negatively affect the overall security of web servers on the network. However, with or without an inventory, the IRS must be vigilant in maintaining adequate security controls over web servers.

On September 14, 2007, the Cybersecurity organization within the MITS issued a comprehensive policy to implement minimum security controls to safeguard internal web servers. In addition to providing configuration guidance on web servers, the policy established roles and responsibilities over web server security. For example, system owners have overall responsibility for the web servers and should work with system administrators to ensure proper server configurations. The system owners' information system security staffs should provide the necessary coordination to ensure that plans for bringing existing web servers into compliance with security procedures are developed and communicated to IRS management. In addition, security specialists in the Cybersecurity organization are responsible for ensuring that system administrators and other personnel having daily operational responsibilities for IRS web servers comply with the security requirements.

Prior to issuance of this specific guidance, the IRS had basic security requirements on server configurations, which included web servers. In general, we found that the new policies and procedures were consistent with the National Institute of Standards and Technology's[10] recommended security controls over web servers.

[10] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

To evaluate compliance with security guidance, we obtained a CSIRC vulnerability scan of web servers conducted in September 2007. This scan identified 2,093 web servers with at least 1 security vulnerability. The scan report contained:

- 540 web servers with at least 1 of 160 high-risk vulnerabilities,
- 1,101 web servers with at least 1 of 117 moderate-risk vulnerabilities, and
- 2,092 web servers with at least 1 of 135 low-risk vulnerabilities.

The number of web servers did not equal 2,093 because most web servers contained at least 1 high-, 1 medium-, and 1 low-risk vulnerability.

Two examples of high-risk security vulnerabilities identified on the 540 web servers were password and buffer overflow weaknesses.[11]

- 62 web servers contained at least 1 high-risk vulnerability involving passwords. Specifically, the web servers had a blank password, did not require a password, and/or had a password that was the same as the username. These vulnerabilities significantly increased the risk that unauthorized users could access the web servers to alter the servers' contents, copy data, install malicious programs for fraudulent purposes, or attack other computers on the network. Attacking other computers could provide access to taxpayer and personally identifiable information.
- 130 web servers contained at least 1 high-risk vulnerability that could allow hackers to exploit a buffer overflow. Buffer overflows cause the software to react in an undesigned manner. A disgruntled employee could exploit buffer overflow vulnerabilities with carefully crafted executable commands as part of the invalid data and gain control over the web server. With full control, the individual could delete or copy the contents of the web server or attack other computers on the network, similar to the effects of password deficiencies discussed above.

Unauthorized servers pose a greater risk because the IRS has no way to ensure that they will be continually configured in accordance with security standards and patched[12] when new vulnerabilities are identified. Malicious hackers or employees could exploit the vulnerabilities on these web servers to manipulate data on the servers or to use the servers as launch points to attack other computers connected to the network.

We believe that these web servers had security weaknesses primarily because employees were not performing their duties as required. Specifically, system owners were not providing overall

[11] Buffer overflows are caused by inputting invalid data into web servers.
[12] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

security emphasis over their own systems to ensure secure configurations, system administrators did not configure or maintain web servers in accordance with security guidance, and security specialists were not monitoring web servers to identify noncompliant servers.

We acknowledge that compliance with security requirements was probably affected by the timing of the issuance of the security policies and procedures for web servers. During our review, security specialists within the Office of Cybersecurity started working with local system administrators and system owners to resolve security weaknesses identified by the September 2007 CSIRC scan of vulnerable web servers. However, another network scan for servers completed in March 2008 showed that, of the 2,093 web servers previously identified with security vulnerabilities from the September 2007 scan, 1,936 still had at least 1 security vulnerability. The March 2008 vulnerability scan report contained 437 web servers with high-risk vulnerabilities and 699 web servers with moderate-risk vulnerabilities. While some improvements have been made, continued efforts are needed to ensure that security vulnerabilities are corrected or mitigated.

In addition to security vulnerabilities on web servers, we were concerned about the number of web software packages being used on the servers. We attempted to obtain a list of web software packages the IRS had approved for its web servers. Officials from the MITS organization informed us that it does not maintain a list of approved web software packages outside of the modernized environment. For the modernized web servers, the Office of Enterprise Architecture has approved three web software packages for use: Microsoft® Internet Information Server, IBM WebSphere® Application Server, and Oracle® web software.

According to IRS web server security policies and procedures, only web server products and platforms identified by the Office of Enterprise Architecture should be used, and products and associated platforms not approved by the Office of Enterprise Architecture require a formal written waiver. The security procedures also provide specific web software security requirements for Microsoft® Internet Information Server, IBM WebSphere® Application Server, Microsoft® .NET Framework, Apache™[13] HTTP Server, and Apache™ Tomcat Server.

The June 2007 CSIRC network scan identified 2,568 potential web servers connected to the IRS network. Among the web software packages included in the 2,568 web servers were:

- Microsoft® Internet Information Server – 1,393.
- Apache™ – 827.
- Oracle® web software – 15.

The remaining 333 web servers were running 30 other web server software packages. Included in the 30 software packages was embedded web software associated with hardware devices.

[13] Apache™ is free software that is typically bundled with most UNIX operating systems and works with other applications including IBM WebSphere® and Oracle® as a component of their application servers. Security policies and procedures over web servers provide configuration guidance for Apache web software.

While having 33 different web server software packages might be justified, we believe that using as few products as possible would limit security risks, such as monitoring for security vulnerabilities due to software deficiencies and patching known security vulnerabilities, and control costs, such as licensing fees, training money, and maintenance costs.

Recommendations

The Chief Information Officer should:

Recommendation 4: Require quarterly network scans of web servers to measure compliance with security requirements. These scan results should be shared with business unit executives as well as local system administrators to ensure timely tracking and resolution of the vulnerabilities. Repeated noncompliance should be referred to managers of the local web administrators for performance evaluation purposes.

> ***Management's Response:*** The Chief Information Officer agreed with this recommendation. The CSIRC will perform quarterly security assessments of web servers to measure compliance with security requirements, and the IRS will review the scans and share the results with business unit executives and local administrators. Business owners and system administrators must eliminate the vulnerabilities.

Recommendation 5: Formally limit the number of approved web software packages for web servers used in the non-modernized environment.

> ***Management's Response:*** The Chief Information Officer agreed with this recommendation. The IRS will investigate the web server packages currently in use and work with the Office of Enterprise Architecture to create a list of approved software. Business owners will be accountable for adhering to the list of approved software.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS is adequately securing and controlling its web servers. The audit focused on the security of internal IRS web servers on the IRS network. To accomplish our objective, we:

I. Determined whether the IRS was properly accounting for and controlling its web servers.

A. Evaluated policies and procedures over the ownership, inventory, and accountability of web servers.

1. Identified IRS policies and procedures over asset management for web servers.

2. Determined compliance with policies and procedures established to ensure that all web servers are identified and controlled.

B. Identified and obtained sources of web server inventory records. We obtained the following sources of information:

1. CSIRC scan report, dated June 2007, that listed 2,568 web servers.

2. CSRIC scan report, dated September 2007, that listed 2,093 web servers.

3. CSRIC scan report, dated March 2008, that listed 1,937 web servers.

4. Enterprise Operations organization spreadsheet, dated October 2007, that included 1,008 web servers.

5. Enterprise Services organization web registration database, dated August 2007, that contained 2,878 active web servers. We validated the reliability and accuracy of the web registration database by comparing it to the CSIRC scan report dated September 2007.

C. Coordinated with the MITS organization to identify ownership, location, business need, and purpose for the 2,093 web servers identified in the September 2007 CSIRC scan.

1. Identified 1,811 unauthorized web servers by matching the September 2007 CSIRC scan results to the web registration database.

2. Coordinated with the Enterprise Operations organization and identified 1,150 web servers not owned by the Enterprise Operations organization and/or registered with the web registration program.

3. Researched the 1,150 web servers on the IRS online Enterprise System Management system[1] to identify contact point and location. We judgmentally selected 19 computers at 3 IRS offices and confirmed whether they were valid computers on the network but were unintentionally running web servers. The three offices visited were the IRS field offices in Dallas, Texas, and Oakland, California, and the National Headquarters in New Carrollton, Maryland. We used a judgmental sample because we did not plan to project the audit results.
4. For those web servers for which ownership could not be identified by the Enterprise Operations organization or our own research, referred the list to the MITS Program Oversight organization to determine the best approach to identify organizations responsible for the web servers.

D. Identified 33 different web software packages connected to the IRS network from the June 2007 CSIRC scan with 2,568 web servers. We used the June 2007 CSIRC scan because the September 2007 CSIRC scan did not include identification of web software packages.

1. Obtained names of approved web software from the Office of Enterprise Architecture and compared them to the list of web software identified in the CSIRC scan of 2,568 web servers.
2. Obtained feedback from the MITS organization on its perspective on web software usage.

II. Determined whether the IRS was adequately securing web servers.

A. Evaluated policies and procedures for security over web servers. We compared Internal Revenue Manual section 10.8.42 v17, entitled Web Server and Web Applications Security, to the National Institute of Standards and Technology[2] *Guide for Assessing the Security Controls in Federal Information Systems* (Special Publication 800-53).

B. Analyzed available vulnerability scans.

1. Identified those web servers that failed the June 2007 and March 2008 CSIRC vulnerability scans with high-, medium-, and/or low-risk vulnerabilities.

[1] The IRS online Enterprise System Management system provides design, development, deployment, and operational support for the enterprise-wide management of IRS computers.
[2] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

2. Determined whether the CSIRC followed up with server owners on web servers with high-risk vulnerabilities, resolved the weaknesses, and identified why the vulnerabilities existed.
3. Determined whether the CSIRC conducted regular scans of the network to identify unauthorized web servers, non-standardized web software, or vulnerable web servers.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Preston B. Benoit, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
David Brown, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Midori Ohno, Senior Auditor
William Simmons, Senior Auditor
Stasha Smith, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, Applications Development OS:CIO:AD
Associate Chief Information Officer, Cybersecurity OS:CIO:C
Associate Chief Information Officer, Enterprise Networks OS:CIO:EN
Associate Chief Information Officer, Enterprise Operations OS:CIO:EO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

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

AUG 11 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez
Chief Information Officer

SUBJECT: Draft Audit Report – Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network (Audit #200720015) (i-trak #2008-39947)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate the report recognizing that the IRS issued a comprehensive security policy on web servers and web software in September 2007 to better identify security controls and requirements for web servers. The policy established minimum security controls to safeguard both internal and external web servers.

The IRS's Modernization and Information Technology Services organization continually strives to improve the security of our information technology resources by ensuring policies are current and TIGTA recommendations are implemented. We agree with, and will implement, all of your recommendations as specified in the attachment.

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment

Attachment

Draft Audit Report – Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network (Audit # 200720015) (i-trak # 2008-39947)

RECOMMENDATION #1: The Chief Information Officer (CIO) should establish official ownership of the web registration program and assign responsibility for the web registration process and the web registration database. Policies and procedures should be updated to reflect the change of ownership.

CORRECTIVE ACTION #1: We agree with this recommendation. The Associate Chief Information Officer, Enterprise Operations was designated the responsible official for the web registration program and web registration database. Policies and procedures will be updated to reflect this.

IMPLEMENTATION DATE: October 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

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 enforce IRS procedures to block unauthorized web servers from providing data over the IRS network. We recognize that some web servers used for legitimate business purposes might be temporarily blocked during this effort. In these instances, web server owners will have to quickly obtain formal authorization and be reconnected to the network. We believe that blocking the unauthorized web servers is the most effective and efficient approach to obtaining an accurate inventory of authorized web servers.

CORRECTIVE ACTION #2: We agree with this recommendation. The IRS will take steps to identify unauthorized web servers and will create a policy and procedure to prohibit them from providing data over the IRS network. We will also establish a process to accommodate legitimate web servers impacted by this recommendation.

IMPLEMENTATION DATE: May 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Chief Information Officer should require an annual scan of web servers and compare the scan results to the web registration database. Unauthorized web servers should be immediately disconnected from the IRS network architecture, and any web site

Attachment

Draft Audit Report – Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network (Audit # 200720015) (i-trak # 2008-39947)

identified with inappropriate content should be referred to the Treasury Inspector General for Tax Administration's Office of Investigations. In addition, owners of registered web servers should be required to revalidate the need for the web servers annually and immediately notify the Chief Information Officer when web servers are decommissioned.

CORRECTIVE ACTION #3: We agree with this recommendation. The Computer Security Incident Response Center (CSIRC) performs recurring discovery and enumeration of enterprise assets. While enterprise discovery efforts are ongoing, CSIRC will provide an annual report to the web registration database business owner to reconcile discovered assets with those currently registered.

The IRS will compare the annual scans run by CSIRC to the web server database and disconnect non-compliant unauthorized web servers. We will refer web sites identified with inappropriate content to the Treasury Inspector General for Tax Administration's Office of Investigations. We will also develop a process to ensure registered web server owners revalidate the need for the web servers annually and provide notification when decommissioned.

IMPLEMENTATION DATE: August 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Information Officer should require annual network scans of web servers to measure compliance with security requirements. These scan results should be shared with business unit executives as well as local system administrators to ensure timely tracking and resolution of the vulnerabilities.

CORRECTIVE ACTION #4: We agree with this recommendation. CSIRC will perform quarterly security assessments of web servers to measure compliance with security requirements. The IRS will review these quarterly scans and share the results with business unit executives and local system administrators. Business owners must support the actions indicated by the scans to eliminate vulnerabilities. Likewise, system administrators must participate in resolving vulnerabilities quickly.

IMPLEMENTATION DATE: August 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.

Attachment

Draft Audit Report – Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network (Audit # 200720015) (i-trak # 2008-39947)

RECOMMENDATION #5: The Chief Information Officer should formally limit the number of approved web software packages for web servers used in the non-modernized environment.

CORRECTIVE ACTION #5: We agree with this recommendation. The IRS will investigate the web software packages currently in use and work with its Enterprise Architecture group to create a list of approved software. Business owners will be accountable for adhering to the approved list.

IMPLEMENTATION DATE: May 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.