Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations

September 18, 2013

Reference Number: 2013-20-106

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

AUTOMATED MONITORING IS NEEDED FOR THE VIRTUAL INFRASTRUCTURE TO ENSURE SECURE CONFIGURATIONS

Highlights

Final Report issued on September 18, 2013

Highlights of Reference Number: 2013-20-106 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Server virtualization is a technology that allows several "virtual" servers to run on one physical host. The conversion of physical servers to virtual servers improves hardware utilization, saves on electricity, and reduces server replacement costs. The IRS has made significant progress in expanding its virtual environment; however, more attention is needed to ensure that configurations are secure. Vulnerabilities in the virtual infrastructure could put taxpayer data at risk of unauthorized disclosure or loss.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to determine whether the IRS's virtual environment is secure.

WHAT TIGTA FOUND

The IRS developed a comprehensive policy that establishes the minimum security controls to prevent unauthorized access to IRS information systems hosted in its virtual environment. A successful attack against a host can compromise all of the virtual servers residing on that host.

TIGTA tested 16 hosts and found that 12 (43 percent) of 28 required security controls were failed by three or more hosts. In addition, 10 (63 percent) of the 16 hosts were missing a total of 48 security patches. The IRS did not use an automated means to check that the security configuration settings were maintained in accordance with the IRS's baseline configuration settings. Also, audit logs for the hosts were not collected and reviewed as required by IRS policy. Until an automated monitoring tool is implemented, the IRS will not be able to effectively monitor and maintain security configurations that are needed to secure the IRS virtual infrastructure and the sensitive data that reside on it.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that the IRS: 1) implements an automated tool to ensure that host and vCenter™ settings remain in compliance with configuration standards; 2) applies patches to hosts timely in accordance with IRS policy; and 3) implements audit log collection and review on hosts and vCenters in accordance with IRS policy.

The IRS agreed with all of TIGTA's recommendations and plans to: 1) procure and/or develop an automated tool, or adapt existing monitoring infrastructure, to report virtual host and vCenter compliance; 2) apply patches to hosts timely in accordance with IRS policy; and 3) develop audit plans and implement log file collection and review for both the hosts and vCenters.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 18, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations (Audit # 201320004)

This report presents the results of our review to determine whether the Internal Revenue Service's virtual environment is secure. This review is part of the Treasury Inspector General for Tax Administration's Fiscal Year 2013 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 VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 5

The Internal Revenue Service Established Policies and Procedures to Expand Server Virtualization and Set Security Standards for Its Virtual Environment ..... Page 5

Automation Will Allow for Better Monitoring of Security on Hosts ..... Page 6

Recommendations 1 and 2: ..... Page 12

Audit Logs Are Not Collected or Reviewed ..... Page 12

Recommendation 3: ..... 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 – Security Configuration Settings and Related Vulnerabilities ..... Page 18

Appendix V – Missing Patches and Related Vulnerabilities ..... Page 20

Appendix VI – Glossary of Terms ..... Page 22

Appendix VII – Management's Response to the Draft Report ..... Page 29

Abbreviations

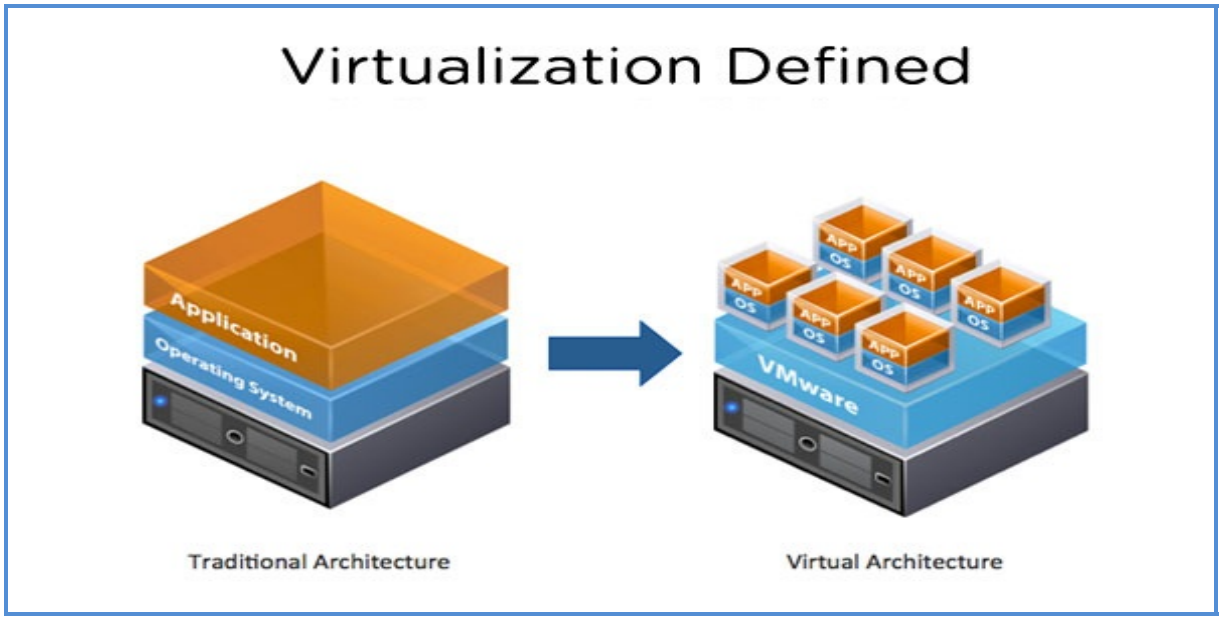
GSS	General Support System
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration
VPO	Virtualization Project Office

Background

Server virtualization is a technology that allows several "virtual" servers[1] to run on one physical host server (hereafter referred to as a "host"), as illustrated in Figure 1. The technology helps organizations use their existing hardware infrastructure more effectively, which:

- Reduces energy and server replacement costs.
- Improves operational efficiency.
- Lowers operational costs through standardization by making it easier to load or remove a server from the operating environment.
- Reduces hardware downtime, provides automatic load balancing, and allows for movement of data before a system failure.

Figure 1: Illustration of Server Virtualization



Source: The VMware® website: http://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works.html.

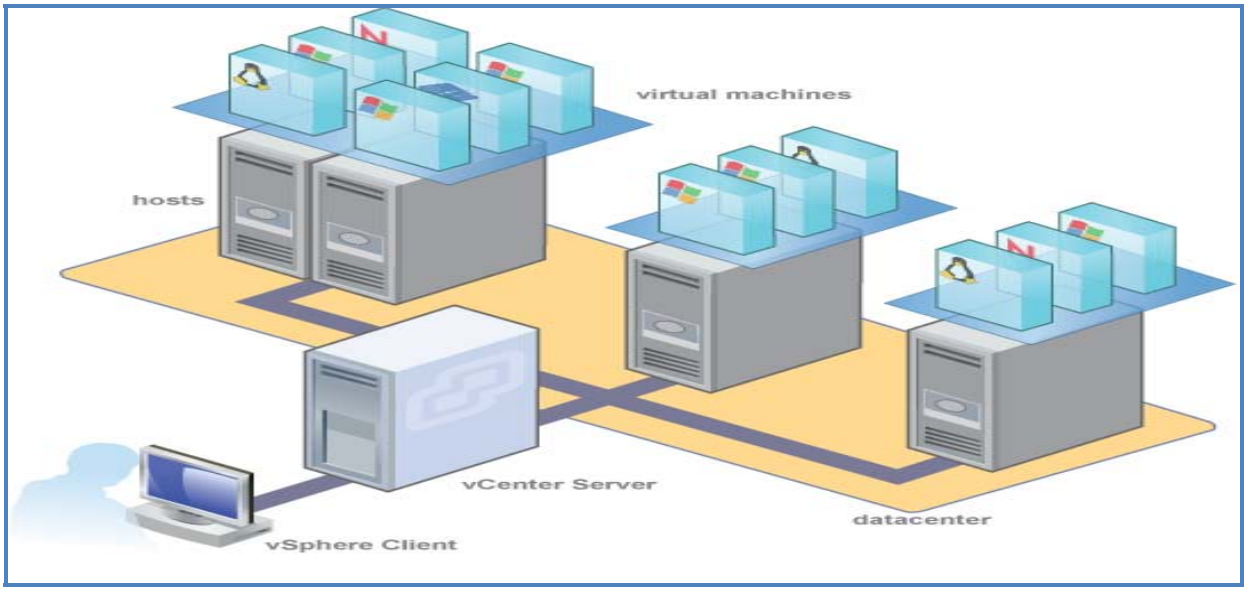
In 2007, the Internal Revenue Service (IRS) concluded that its diverse and widely deployed server infrastructure would benefit from a consolidation and virtualization project. That same

[1] See Appendix VI for a glossary of terms.

year, the IRS established the Virtualization Project Office (VPO) to design and implement a virtual infrastructure using VMware® ESX virtualization software (VMware) to facilitate the consolidation and virtualization of its x86-based systems. The IRS's virtual infrastructure is known as the Virtual Host Infrastructure, hereafter referred to as General Support System 39 (GSS-39).

The VMware infrastructure (also referred to as "vSphere") uses a centralized management tool called the Virtual Center (vCenter™), which provides essential data center services such as access control, performance monitoring, and configuration management. It provides system administrators with simple and automated control over the virtual environment.

Figure 2: VMware Basic Components and Their Relationship to Each Other



Source: Host illustration within the IRS VMware vSphere vCenter.

A thin layer of the virtualization software called a hypervisor runs on the host and dynamically allocates computing resources to each virtual server as needed. The hypervisor has improved reliability and security due to fewer lines of code than traditional operating systems for physical systems. This drastically reduces the risk of bugs or security vulnerabilities and makes it easier to secure the host. This also simplifies host patching and updating due to its smaller size and fewer components.

In a 2012 Forrester report, security specialists warn that "Virtualization brings new layers that we must secure. We have additional infrastructure and management layers to protect, as well as the hypervisor itself. If an insider or cybercriminal compromises either, all bets are off."[2] For

[2] Rick Holland, Forrester Research Inc., *The CISO's Guide to Virtualization Security* (Jan. 12, 2012).

instance, the hypervisor running on the host creates a new attack surface in the virtual environment. The hypervisor provides a single point of access into the virtual environment and is also potentially a single point of failure. Misconfigured hypervisors could result in a single point of compromise for the security of all hosted components. No matter how securely the individual virtual servers or components may be configured, a compromised hypervisor can override those controls and gain direct access to the virtual systems. In a similar manner, the security of a vCenter is paramount to the overall security posture of the virtual environment. Compromise of the vCenter could potentially lead to complete ownership of the hosts, virtual servers, and virtual networks by an attacker.

The GSS-39 provides the virtual infrastructure for the majority of the IRS's virtual servers. Other IRS organizations have implemented virtual infrastructure to maintain virtual servers and hosts of their own, including Criminal Investigation; the Research, Analysis, and Statistics organization; and the Development, Integration, and Test Environment organization. Figure 3 below contains current virtual server and host inventory figures for the various organizations as of March 2013.[3] Because the majority of virtual servers and hosts reside on the GSS-39 infrastructure, we limited our review to that environment.

Figure 3: IRS Virtual Servers and Host Inventory

Virtual Server and Host Inventory		
Organization	**Virtual Servers**	**Hosts**
Information Technology (GSS-39)	5,175	328
Development, Integration, and Test Environment	395	74
Criminal Investigation	210	35
Research, Analysis, and Statistics	17	5
Total	**5,797**	**442**

Source: Inventory data were provided by Criminal Investigation and the Information Technology; Research, Analysis, and Statistics; and Development, Integration, and Test Environment organizations.

In March 2012, the Treasury Inspector General for Tax Administration (TIGTA) reported[4] that the IRS had successfully implemented server virtualization technology to improve server efficiency and realize cost savings. TIGTA recommended that the IRS further expand its

[3] All inventory information is as of March 2013 except the Development, Integration, and Test Environment organization information, which is as of April 2013, and the Criminal Investigation information, which is as of August 2013.
[4] TIGTA, Ref. No. 2012-20-029, *Virtual Server Technology Has Been Successfully Implemented, but Additional Actions Are Needed to Further Reduce the Number of Servers and Increase Savings* (Mar. 2012).

virtualization efforts by identifying servers located in field offices and virtualizing those servers as well. At the end of Fiscal Year 2011, the IRS had approximately 1,800 virtual servers operating on 234 physical host servers in the GSS-39 virtual environment and estimated that it saved $10.2 million in equipment costs over two years through server virtualization. Also, the IRS expected to save approximately $1.3 million annually in decreased electrical costs beginning in Fiscal Year 2013. By virtualizing servers in the field offices, the IRS estimated that it could realize additional savings of approximately $7.73 million ($7.26 million in equipment savings and $470,000 in electrical savings over five years).

This review was performed at the offices of the Information Technology organization in New Carrollton, Maryland; Martinsburg, West Virginia; and Ogden, Utah, during the period October 2012 through July 2013. 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

The Internal Revenue Service Established Policies and Procedures to Expand Server Virtualization and Set Security Standards for Its Virtual Environment

The 2012 Forrester report stated, "IT [Information Technology] professionals have virtualized, on an average, fifty-two percent of the x86 servers in enterprise environments; in two years, they expect that number to grow to seventy-five percent." The IRS has successfully continued to expand its virtual environment. The IRS established a policy that IRS organizations must virtualize all physical servers unless it would be economically unfeasible to do so.

According to Forrester 2012 survey data, information technology professionals have virtualized, on average, 52 percent of the x86 servers in enterprise environments; in two years, they expect that number to grow to 75 percent.

In May 2012, the VPO was managing the GSS-39 virtual server environment with 3,271 virtual servers running on 351 physical host servers at 13 data centers, resulting in hardware savings in excess of $20 million. At that time, the virtual environment represented 39 percent of the x86 Windows environment. As of June 2013, the GSS-39 x86 virtualization statistics have significantly improved, showing a total of 328 hosts and 5,399 virtual servers (or 16.46 virtual servers per host) and achieving over 54 percent overall virtualization and over $51 million in estimated cost savings.[5]

The VPO has established management processes for expanding and monitoring the GSS-39 virtual environment, such as:

- Tracking requests from IRS organizations for setup of new virtual servers.
- Tracking problem tickets for resolving virtual system problems.
- Performing daily manual checks of the virtual environment by the system administrators who monitor information through the vCenters regarding virtual server health, computer processing usage, and other operational issues.

[5] Estimated cost savings are based upon a comparison of using virtual server configurations versus the purchase of new physical servers.

- Maintaining a document library on a Virtualization SharePoint that contains GSS-39 architectural documents, security requirements, VMware vendor documentation and guides, training videos, and Frequently Asked Questions.
- Monitoring configuration settings of vCenter servers (which run on the Windows operating system) using Windows Policy Checker scans. Our review of Windows Policy Checker scans run in March 2013 on all eight GSS-39 vCenter servers reported that seven of the eight had an overall compliance rate of 98.56 percent and the remaining one had an overall compliance rate of 96 percent.

In addition, the IRS developed a comprehensive policy that defines the minimum security controls needed to safeguard its virtual environment. The purpose of the policy is to protect its critical infrastructure and assets against attacks that exploit virtualization and to prevent unauthorized access to IRS information systems hosted in the virtual environment. The policy is consistent with guidelines issued by the National Institute of Standards and Technology, the Defense Information Systems Agency, the Center for Internet Security, VMware, and other industry best practices. The policy also defines the roles and responsibilities that are specific to the implementation of the IRS virtual environment.

The IRS has been successful in its continual efforts to expand its virtual environment. As a result, the IRS has improved server efficiency and realized significant cost savings. However, as the IRS continues on this course, and more IRS data are maintained in its virtual environment, the IRS must remain vigilant in regard to virtual security. The Forrester report states, "The technology is mature and enterprise adoption is high, yet information security does not have a significant focus on virtual security." The IRS must strive to increase the security maturity of its virtual environment and not allow it to lag behind operations.

According to Forrester, the technology is mature and enterprise adoption is high, yet information security does not have a significant focus on virtual security.

Automation Will Allow for Better Monitoring of Security on Hosts

Although the VPO has established processes to monitor its virtual infrastructure, we found that security configuration settings on hosts were not in accordance with IRS policy. In addition, the hosts were not timely patched to address known security vulnerabilities.

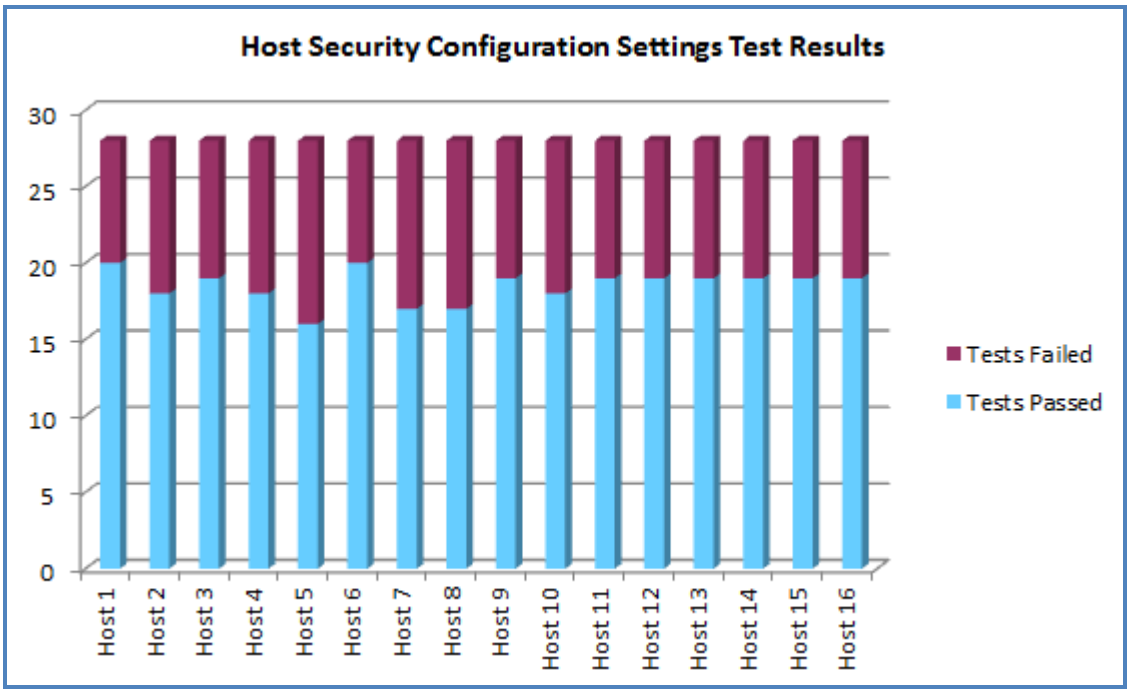
Host security configuration settings were not in accordance with IRS policy

IRS policy requires hosts to be configured in accordance with the latest security hardening guide.[6] To test whether GSS-39 hosts were in compliance with security configurations, we

[6] The latest hardening guide at the time of this review was the vSphere 5.0 Security Hardening Guide. This guide provides information about securing vSphere components, including the hosts and vCenters.

selected 16 hosts that had been recently upgraded to vSphere 5.0[7] and compared their settings with the VMware vSphere 5.0 Security Hardening Guide. We tested 28 security configuration settings that were applicable to the GSS-39 environment and should have been set in accordance with the security hardening guide. We found that all 16 hosts were in compliance with 16 (57 percent) of the 28 settings we tested. Conversely, we also found that three or more of the 16 hosts failed each of the remaining 12 (43 percent) of the 28 settings. Figure 4 below illustrates that the 16 hosts were configured inconsistently during their recent upgrade, in that the number of configurations that each passed or failed varied.

Figure 4: Graphical Depiction of Security Configuration Setting Compliance for 16 Hosts Reviewed by TIGTA



Source: TIGTA review of 28 security configuration settings on 16 hosts.

Each of the 12 failed settings previously mentioned is presented in Figure 5, along with the number and percentage of hosts that failed.

[7] On March 25, 2013, the IRS began upgrading the hosts in the GSS-39 infrastructure from vSphere ESXi 4.1 to 5.0 update 2. As of July 8, 2013, the process is 93.23 percent complete.

Figure 5: Configuration Settings Failed By 16 Hosts

Configuration Setting	No. of Hosts That Failed	Percentage of Hosts Tested
**********2********** **********2**********	16	100%
**********2**********	16	100%
**********2********** **********2**********	16	100%
**********2**********	16	100%
**********2********** ********2**********	16	100%
**********2********** **********2**********	16	100%
**********2********** **********2**********	16	100%
**********2**********	16	100%
**********2**********	10	63%
**********2**********	7	44%
**********2**********	4	25%
**********2**********	3	19%

Source: TIGTA review of security configuration settings on 16 hosts. Percentages are derived by dividing the number of hosts that failed by the total number of hosts reviewed.

Although IRS policy requires administrators to configure hosts in accordance with the latest hardening guide, the administrators were not ensuring that hosts were properly configured.
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
****

**********2**********
**********2**********

**********2**********
**********2**********
**********2**********.

A feature within the vCenters called host profiles can reduce the manual steps that are involved in configuring a host and can help maintain consistency and correctness of configuration settings. It can provide information about the configuration compliance of the hosts. It checks that a host's configuration matches the configurations specified by policy. Host profiles can also be set to send alerts when configurations are not in compliance. However, host profiles are limited in regard to the configurations that can be set. For example, only five of the 12 failed security configuration settings above could be set by host profiles.

However, host profiles could have been used to properly configure**********2**********
**********2**********
**********2**********
**********2**********. Although the VPO had supplied the host administrators with upgrade procedures that included instructions on checking compliance through host profiles, our results show that not all administrators were using host profiles to ensure consistency and correctness of configuration settings.

Patches were not applied in a timely manner

Newly upgraded hosts were not always brought up to date with patches. Our test results indicated that 10 (63 percent) of the 16 recently upgraded hosts still had missing patches. We identified 48 missing patches on the 10 hosts. Of the 48 missing patches, nine were critical,[8] 38 were high, and one was medium. Patches had been missing from 21 days up to 167 days. Of the critical patches, two had been missing 167 days and seven had been missing 69 days.

The VPO halted patching on hosts in December 2012 until upgrades were completed, stating that all their efforts were on the installation of the upgrades. The VPO intended that hosts would be fully patched as each was newly configured during the upgrade. The VPO estimated that the upgrade would be fully deployed by August 2013.

IRS policy requires that virtualized computing environments be kept current with all applicable server software patches, hotfixes, and updates. IRS policy also sets forth criteria for implementing patches in a timely manner. It states that distribution of patches with a priority of critical shall begin within 72 hours of patch availability, distribution of patches with a priority of high shall begin within five business days of patch availability, and distribution of patches with a priority of medium shall begin within 30 calendar days of patch availability.

Not installing security patches in a timely fashion puts the IRS at risk that known vulnerabilities in systems may be exploited. An unpatched vulnerability at the host level could allow an

[8] A critical patch fixes flaws in a product that can potentially cause data loss or severe service disruption.

attacker to gain access to the host and from there take over the virtual servers that reside on it, putting sensitive IRS data contained in the virtual servers at risk of disclosure or loss.

Examples of ***2**** on the newly upgraded hosts included:

- **********2**********2**********.
- **********2**********2**********2**********2**********.
- **********2**********2**********2**********2**********.

Appendix V provides a full listing of the missing patches from our review of the 16 recently upgraded hosts and describes the potential risks if they are not installed timely on the hosts. Subsequent to our review of the 16 hosts, the IRS has indicated that it has installed the missing patches on the hosts.

The deficient security configuration settings and missing patches could have been discovered and corrected if the VPO had an automated means to fully check all required settings and patches, both immediately following the upgrade and periodically in the future. IRS policy states that automated means must be employed to check that security configurations are continually maintained in accordance with IRS requirements. In addition, a means to automate enforcement of selected configurations must be implemented. Further, automated scanning of operating systems must be conducted at a minimum of monthly.

The VPO informed us that it is in the process of purchasing a tool called Quest vFoglight,[9] which is an automated performance monitoring and capacity management tool. This management tool will enable it to perform an analysis of the capacity of VMware infrastructure to make determinations of what excess capacity remains and perform accurate capacity forecasts. Also, it would provide capabilities to monitor and alert the host administrator when security configurations change. Baseline configuration settings based on the security hardening guide could be established, which the tool will then monitor and send an alert if settings change. However, the VPO has not implemented the tool yet because use of the tool has not completed the IRS approval process.

In the interim, the VPO could employ a free tool available through VMware that can scan hosts and provide an automated means to check security configuration settings against the security hardening guide. VMware also offers free tools that can scan other components of the virtual

[9] Dell Inc. acquired Quest Software on September 28, 2012.

infrastructure, such as the vCenter servers and the virtual network. If using the VMware tool is not feasible for the IRS environment, the VPO could develop scripts to automate the monitoring of the host security configuration settings, just like the script it developed to check the network time protocol time server and report any host that did not comply with the standard time.

When security configuration settings are not in place, vulnerabilities exist that leave the GSS-39 environment less secure. Weaknesses in the host's security hardening and patching could be identified and exploited, allowing attackers to gain access to individual virtual servers and any sensitive data they contain. **********2*********:

- **********2**********.
- **********2**********2**********.
- **********2**********.
- **********2**********.
- **********2**********.
- **********2**********2**********.

Appendix IV lists all 12 failed security configuration settings and describes the vulnerabilities that result from not ensuring that they are properly set. Until an adequate automated monitoring tool is implemented, the IRS will not be able to effectively monitor and maintain security configurations that are needed to secure the IRS virtual infrastructure and the sensitive data that resides on it.

Recommendations

The Chief Technology Officer should ensure that the IRS:

Recommendation 1: Implements an automated management tool to ensure that host and vCenter settings remain in compliance with configuration standards.

Management's Response: The IRS agreed with this recommendation. The IRS will procure and/or develop an automated tool, or adapt existing monitoring infrastructure, to report virtual host and vCenter compliance.

Recommendation 2: Applies patches to hosts timely in accordance with IRS policy.

Management's Response: The IRS agreed with this recommendation. The IRS will apply patches to hosts timely in accordance with IRS policy.

Audit Logs Are Not Collected or Reviewed

Audit logs that capture administrator activity on GSS-39 hosts and vCenter servers were not collected and reviewed as required by IRS policy. IRS policy requires the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. Auditable events must be captured for all IRS systems.

IRS information technology security specialists are assigned the responsibility to review audit information, including review of audit logs after an event and scheduled reviews at least weekly at the discretion of the information system owner. Automated software tools must be used to provide audit log reduction and reporting capabilities in accordance with an approved audit plan. Administrators of IRS systems must implement the necessary software configuration changes and install the necessary software tools to bring IRS systems into compliance with the requirements.

Quest InTrust, the tool used by the IRS Enterprise Operations' Security Operations Management organization to collect the audit logs and make them more usable for review, did not have the capability to collect host and vCenter logs until August 2012. When the capability was available, the VPO did not provide the credentials (login and password with an elevated type of privilege) to the Security Operations Management organization that were necessary to establish the logging process.

After TIGTA brought this issue to the VPO's attention, the VPO took actions to provide the credentials needed for the Quest InTrust staff to begin collecting audit logs from the vCenters. At the time of our review, the Quest InTrust staff was planning to test whether their log collection efforts were successful. However, the VPO did not agree that the host logs needed to be collected and reviewed by the Quest InTrust team. The VPO indicated that the host logs were currently collected by a virtual appliance and mainly leveraged for diagnostics for technical support.

However, IRS policy requires that audit logs maintain a record of user activity and provide a means to establish individual accountability. In addition, IRS policy requires that audit logs be collected in a secure, centralized location that prevents log tampering, where events can be properly reviewed and analyzed by IRS security specialists. Without adequate audit logs, the

IRS may be unable to identify or substantiate unauthorized or improper activity or to hold individuals accountable for the actions taken. **********2********** **********2**********.

Without the proper capture and review of administrator activity, accountability for actions taken on hosts cannot be established and unauthorized activity may go undetected. Moreover, the IRS could have a security breach in the virtual environment and not be aware of it. Without sufficient audit logs, it may not be possible to develop the details necessary to understand how breaches occurred or how long they have been present or, in the case of investigators, to develop all the details needed to support a civil or criminal case.

Subsequent to the completion of our fieldwork, the IRS informed us that it has begun collecting audit logs for the vCenters in the Quest InTrust repository and has begun testing audit log collection for the hosts. The IRS also informed us that its next steps include developing audit plans for both the vCenters and the hosts to ensure proper events are logged.

Recommendation

The Chief Technology Officer should ensure that the IRS:

Recommendation 3: Implements audit log collection and review on hosts and vCenters in accordance with IRS policy, including logging when users access these devices, the logon and logoff times, and the activities conducted during access.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization will develop an audit plan and implement virtual log file collection and review for both the vCenter and virtual infrastructure host servers. The IRS indicated it currently has an interim process in place to collect virtual host and vCenter log files.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS's virtual environment is secure. To accomplish the objective, we:

I. Evaluated the IRS's enterprisewide virtual environment and the impact of a software upgrade on security controls.

A. Gathered documentation for the IRS enterprise virtual environment and interviewed the IRS Information Technology staff, including Enterprise Operations and Cybersecurity staffs.

B. Reviewed documentation on the virtualized SharePoint that included network maps/diagrams, security documents, vCenter information, and other supporting documentation that verifies the secure setup of the entire virtual environment, including management, storage, and network components.

II. Determined if adequate controls have been established to properly and securely manage the virtual environment.

A. Determined if adequate policies, procedures, roles, and responsibilities for the management of the virtual environment had been established.

B. Evaluated how tools are used to monitor the virtual infrastructure to ensure consistent and secure host and vCenter server configurations. To determine if security configuration settings were in compliance with IRS policy, we selected a sample of 16 hosts from the population of 222 hosts that had been recently upgraded to vSphere 5.0. We judgmentally selected the 16 host servers due to time constraints and the time-intensive process required to manually determine if security settings were in compliance with the hardening guide. A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population. We also selected all eight vCenters and reviewed their May 2013 Windows Policy Checker scan reports.

C. Determined if the hardware capacity is being effectively managed in order for the virtual environment to support existing and future business requirements.

D. Determined if adequate port scanning and vulnerability remediation processes were in place. We interviewed Cybersecurity and Enterprise Operations staffs on the status of the enterprisewide vulnerability scanning and remediation process and its coverage

of the virtual environment. We did not evaluate the nCircle data because, during the planning phase of the audit, we determined that the nCircle data were inaccurate.

III. Determined if adequate security controls were in place to ensure hosts and the virtual management network was secured.

A. Evaluated access and privileged user management controls.

B. Evaluated audit logging controls by interviewing personnel in the VPO and the Cybersecurity office. We did not review audit logs because audit logs were not yet being collected.

C. Evaluated data backup controls and disaster recovery procedures.

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 the following internal controls were relevant to our audit objective: IRS policy and procedures for securing virtual environments within the IRS and its monitoring processes for ensuring controls remain effective. We evaluated these controls by reviewing industry guidance related to virtualization; Internal Revenue Manual 10.8.9, *Information Technology (IT) Security, Virtualization Security Policy*; and other relevant IRS standard operating procedures. We also interviewed IRS Information Technology management in the Enterprise Operations organization with duties related to the IRS's virtual environment. We also observed security configuration settings on host and vCenter servers located in Martinsburg, West Virginia, and Ogden, Utah.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Esther Wilson, Senior Auditor
Sam Mettauer, Information Technology Specialist
Larry Reimer, Information Technology Specialist

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Office of the Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner for Operations Support OS
Chief Technology Officer OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO: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: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Security Configuration Settings and Related Vulnerabilities

Security Configuration Setting	Vulnerability
**********2********* **********2********* **********2*******	**********2********** **********2********** **********2**********
**********2********* ****2******	**********2********** **********2********** **********2********** **********2********** **********2********** **********2**********.
*********2********** *********2********** *********2********** *2*********	**********2********** **********2********** **********2********** ***********2**********.
*********2********** *********2**********	**********2********** **********2********** **********2********** **********2********** **********2********** ***********2**********.
**********2********** *********2********** ******2*********	**********2********** **********2********** **********2**********
********2********** *********2********** *********2**********	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2**********.

Security Configuration Setting	Vulnerability
**********2********** **********2********** **********2********** ******2*******	**********2********** **********2********** **********2**********.
**********2********** **********2**********	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2**********
****2**********	**********2********** **********2********** **********2**********.
**********2********** **********2*********	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** ********2****
*********2********** *******2****	**********2********** **********2********** **********2********** **********2********** **********2********** **********.
**********2********* ******2*******	**********2********** **********2********** *********2**********.

Source: The VMware vSphere 5.0 Security Hardening Guide, version 1.2, dated December 18, 2012.

Appendix V

Missing Patches and Related Vulnerabilities

	Patch	Date Issued	Severity	Patch/Vulnerability Description	Total Missing
1.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2**********.	10
2.	**********2*********	**2**	**2**	**********2********** **********2**********	7
3.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2**********	7
4.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2**********	7
5.	**********2*********	**2**	**2**	. **********2********** ********2*******	7
6.	**********2*********	**2**	**2**	**********2********** ******2*******	1
7.	**********2*********	**2**	**2**	**********2********** **********2********** **********2**********	1
8.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2**********	1

	Patch	Date Issued	Severity	Patch/Vulnerability Description	Total Missing
9.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** ******2*********	1
10.	**********2*********	**2**	**2**	**********2********** **********2**********	1
11.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** *********2**********	1
12.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********	1
13.	**********2*********	**2**	**2**	**********2********** **********2********** **********2********** **********2**********	1
14.	**********2*********	**2**	**2**	**********2********** **********2********** ******2**********	1
15.	**********2*********	**2**	**2**	. **********2********** **********2********** **********2********	1
				Total Missing Patches on Hosts:	**48**

Appendix VI

Glossary of Terms

Term	Definition
Access Control	Access control ensures that resources are only granted to those users who are entitled to them.
Active Directory	A Microsoft Corporation software system for administering and securing computer networks. Active Directory manages the identities and relationships of computing resources that comprise a network. It enables administrators to assign enterprisewide policies, deploy programs to many computers, and apply critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.
Agent	A software routine that waits in the background and performs an action when a specified event occurs. For example, a restarting agent would resume operations after a planned or unplanned termination.
Alert	A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.
Application	Any data entry, update, query, report, or program that processes data for the user.
Application Programming Interface	Specifies how some software components should interact with each other.
Arbitrary Code Execution	Used to describe an attacker's ability to execute any commands of the attacker's choice on a target machine or in a target process.
Attack	An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures.
Audit Log (or Audit Trail)	In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and any actual or attempted security violations that occurred, both legitimate and unauthorized.
Audit Plan	Used as guidance for the implementation of configuration-specific audit settings for the operating systems and software for which they are intended.

Term	Definition
Auditing	A review and analysis of management, operational, and technical controls. The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system.
Authenticate (and Authentication)	To establish the validity of a claimed user or object by positively verifying the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Bandwidth	The transmission capacity of an electronic pathway such as a communications line, computer bus, or computer channel. Digital bandwidth is the number of pulses per second measured in bits per second.
Best Practice	A technique or methodology that, through experience and research, has proven to reliably lead to a desired result.
Boot	Causes the computer to start executing instructions.
Buffer Overflow	Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. In buffer overflow attacks, the extra data may contain codes that could damage user files, change data, or disclose confidential information.
Bug	An error or defect in software or hardware that causes a program to malfunction.
Capacity Management (or Planning)	Determining the required future configuration of hardware and software for a network, data center, or website. There are numerous capacity planning tools on the market used to monitor and analyze the performance of the current hardware and software. However, capacity planning also requires insightful forecasting: what if traffic triples overnight, what if a company merger occurs, *etc*. As a result of all the analyses and forecasts, systems can be upgraded to allow for the projected traffic or be enhanced so that they can be ready for a quick changeover when required.
Certificate	A form of digital identification that is used to authenticate Web applications.
Certificate Authority	A trusted entity in a public key infrastructure that issues and revokes certificates to ensure compliance to a public key infrastructure policy.
Configuration	The functional and physical characteristics of existing or planned hardware, firmware, or software or a combination thereof as set forth in technical documentation and achieved in a product.
Configuration Setting (or Security Setting)	The set of parameters that can be changed in hardware, software, and firmware that affect the security posture and functionality of the information system.
Data Store	A permanent storehouse of data. The term is often used to lump the storage of all types of data structures (files, databases, text documents, *etc.*) into one generic category.
Denial of Service	Actions that strive to make a computer resource unavailable to authorized users, generally consisting of the concerted efforts of an attacker to prevent an information resource from functioning efficiently or at all, temporarily or indefinitely.

Term	Definition
Disable Direct Console User Interface	Allows for low-level host configuration such as configuring IP [Internet Protocol] addresses, hostnames, and root passwords as well as diagnostic capabilities such as enabling the host shell, viewing log files, and resetting configurations. Actions performed from the Disable Direct Console User Interface are not tracked by the vCenter server. Even if lockdown mode is enabled, someone with the root password can perform administrative tasks in the Disable Direct Console User Interface, bypassing role-based access controls and auditing controls provided through the vCenter. Disabling the Disable Direct Console User Interface prevents all local activity and thus forces actions to be performed in the vCenter, where they can be centrally audited and monitored.
Driver	A program that interacts with a particular device or special kind of software. The driver contains the special knowledge of the device or special software interface that programs using the driver do not.
Elevated Privilege (or Privileged Access)	Any user right assignment that is above the baseline.
Event	Any action that happens on a computer system. Examples include logging in to a system, executing a program, and opening a file.
Firewall	A system designed to prevent unauthorized access to or from a private network.
Firmware	Software instructions residing in nonvolatile memory chips that hold their content without power. Firmware is found on computer motherboards to hold hardware settings and booting data and on myriad consumer electronics devices to hold the operating system or control program.
General Support System (GSS)	An interconnected set of information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people.
Guest Operating System	An operating system running within a virtual server.
Host Operating System	An operating system that runs on the host machine.
Host Profiles	A feature that simplifies host configuration management through user-defined configuration policies. The host profile policies capture the blueprint of a known, validated host configuration and use this configuration to configure networking, storage, security, and other settings across multiple hosts. The host profile policies also monitor compliance to standard host configuration settings across the data center.
Host Server (or Host)	The physical machine that uses a hypervisor to manage the virtual server(s).
Hotfix	A single, cumulative package that includes one or more files that are used to address a problem in a product.
Hypervisor	The virtualization component that manages the guest operating systems on a host and controls the flow of instructions between the guest operating systems and the physical hardware. Also described as software that allows a single host to run one or more guest operating systems. It can also be referred to as a virtual machine manager.

Term	Definition
Identity	Identity is who someone is or what something is; for example, the name by which something is known.
Infrastructure	The fundamental structure of a system or organization. The basic, fundamental architecture of any system (electronic, mechanical, social, political, *etc.*) determines how it functions and how flexible it is to meet future requirements.
Intel	Intel Corporation, in Santa Clara, California, is the largest semiconductor manufacturing company. It is also a leading vendor in computer, networking, and communications products.
Local area network	A communications network that is typically confined to a building or premises.
Lockdown Mode	When a host is in lockdown mode, no user other than the vpxuser has authentication permission, nor can any user perform operations against the host directly. Lockdown mode forces all operations to be performed through the vCenter server. The vpxuser is an account created by the vCenter server when a host is added.
Man-in-the-Middle Attack	An attack that intercepts a communication between two systems.
Managed Object Browser	A graphical interface that allows you to navigate the objects on a server and to invoke methods. Any changes you make through the managed object browser take effect on the server.
Network File Copy	The name of the mechanism used to migrate or make a copy of a virtual server between two hosts over the network.
Network Interface Card	An expansion card (physical or virtual) that provides a dedicated connection between a computer and a network. Also called a network adapter.
Network Time Protocol	A protocol designed to synchronize the clocks of computers over a network.
Operating System	The master control program that runs a computer. The most important program process on a computer because it runs other programs. Operating systems also are responsible for security, such as ensuring that unauthorized users do not access the system.
Password	A secret word or code used to serve as a security measure against unauthorized access to data. It may be used to log on to a computer, network, or website or to activate newly installed software in the computer.
Patch	A small file that when executed will patch or fix specific problems in a target file or application.
Remote Access	Access by users (or information systems) communicating from an external location to an information system security perimeter.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of the likelihood of the circumstance or event occurring and of the resulting adverse impacts.
Root	To enable the highest privilege level and have access to all of a computer's resources.

Term	Definition
Secure Shell	A protocol originally designed to provide a secure alternative to network terminal sessions.
Secure Sockets Layer	The leading security protocol on the Internet used to do three things: validate the identity of a website; create an encrypted connection for sending credit card and other personal data; and ensure that the received data were sent without error.
Security Controls	The management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Hardening Guide	A prescriptive guidance for customers on how to deploy VMware products in a secure manner. It also provides script examples and other information to help with security automation.
Security Requirements	Requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Sensitive Data (or Information)	Information that 1) the loss of, misuse of, unauthorized access to, or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act) but 2) has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy.
Server	A system capable of managing and running virtual machines. Also a process capable of accepting and running instructions from another process.
Setting	A configuration value or rule that determines the behavior of a specific entity or set of entities, such as an application feature.
SharePoint	Used to set up internal Web portals (intranets) for document sharing and search, team collaboration, blogs, and company news.
Shell	The outer layer of a program that provides the user interface, or way of commanding the computer.
Sniff	To look at network traffic as it is being transmitted. The network packets may be analyzed in real time or stored for later inspection.
System Administrator	An individual employed to maintain and operate the technical aspects of an information system. Usually charged with installing, supporting, and maintaining servers or other computer systems and planning for and responding to service outages and other problems.
Translation Lookaside Buffer	A cache (*i.e.*, a component that transparently stores data so that future requests for that data can be served faster) that memory management hardware uses to improve the speed at which a virtual address is translated to a physical address.

Term	Definition
Trusted Execution Technology	A computer hardware technology whose primary goals are to: 1) attest to the authenticity of a platform and its operating system (attestation), 2) assure that an authentic operating system starts in a trusted environment and thus can be considered a trusted operating system, and 3) provide the trusted operating system with additional security capabilities not available to an unproven operating system. The Trusted Platform Module is required to use this technology.
Trusted Platform Module	A specialized chip that can be installed on the motherboard of a personal computer for the purpose of hardware authentication. It authenticates the computer in question rather than the user. To do so, it stores information specific to the host system, such as encryption keys, digital certificates, and passwords. A Trusted Platform Module minimizes the risk that data on the computer will be compromised by physical theft or an attack by an external hacker.
Version	An initial release or re-release of a product.
Virtual Appliance	A software solution that is composed of one or more virtual machines.
Virtual Center (or vCenter)	A centralized console for managing virtual machines and hosts.
Virtual Environment	The physical system running a host operating system and hypervisor, which manages virtual servers that run guest operating systems.
Virtual Infrastructure	The specific hardware solutions and Commercial Off-The-Shelf (that is, ready-made merchandise that is available for sale) tools provided by the GSS-39 and used to facilitate the running of x86 systems, including (but not limited to) the host server, hypervisor, and vCenter.
Virtual Machine (or Virtual Server)	A simulated environment created by virtualization, also described as a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer.
Virtual Network	A network of virtual servers running on a single physical machine that are connected logically to each other so that they can send data to and receive data from each other.
Virtualization	The simulation of the software and hardware upon which other software runs.
Virtualization Project Office	An IRS office established in 2007 to design and implement an enterprisewide virtual environment.
VMkernel	In ESX/ESXi, a high-performance operating system that occupies the virtualization layer and manages most of the physical resources on the hardware, including memory, physical processors, storage, and networking controllers.
VMware ESX/ESXi	Enterprise-level computer virtualization products offered by VMware Inc., developer of virtualization software. Both are a bare metal hypervisor architecture, which means that the hypervisor is installed directly on the server hardware and directly controls the hardware without using device drivers from another operating system.

Term	Definition
VMware Tools	An optional, free set of drivers and utilities that enhances both the performance of a virtual machine's guest operating systems and interaction between the guests and the host.
VMware vSphere	VMware virtualization platform used for building cloud infrastructures. It virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the data center.
vSphere Authentication Proxy	Enables ESXi hosts to join a domain without using Active Directory credentials.
Vulnerability	Flaw or weakness in an information system's design, implementation, or operation and management that could potentially be exploited by a threat to gain unauthorized access to information, disrupt critical processing, or otherwise violate the system's security policy.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.
Windows	The most widely used operating system for desktop and laptop computers. Developed by Microsoft, Windows primarily runs on x86-based systems.
Windows Policy Checker	An automated tool that reads the security settings of computers and logs any noncompliant settings to text files.
X86-Based System	A computer system that is based on Intel's x86 family of microprocessors.

Appendix VII

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

September 9, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – TIGTA Draft Report - Automated Monitoring is Needed on Virtual Infrastructure to Ensure Secure Configurations (Audit # 201320004)

Thank you for the opportunity to review and respond to the subject audit report.

We appreciate your recognition that the Service has improved server efficiency and has realized significant cost savings at this stage of migrating to a virtual server environment. We also are gratified that you found our policies and operational practices consistent with guidelines issued by the National Institute of Standards and Technology, the Defense Information Systems Agency, the Center for Internet Security, VMware, and other industry best practices. We are confident that our routine support practices for our virtual server environment are providing a sound operating environment.

We agree with the recommendations presented in the Draft Report. During the audit, you witnessed our efforts to implement a major upgrade of the Virtual Host Infrastructure including the ESX 4 to ESXi 5 OS/Hypervisor upgrade, firmware upgrades, Storage Systems migration, and configuration upgrades. Because of the dynamic nature of such a major upgrade, we suspended some of our routine support practices and focused our resources on completing our upgrades in as short a time as possible. Once the upgrade is complete, we will not only resume our practices, but will also implement improvements to our support practices based on your suggestions.

We value your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 622-6800, or a member of your staff may contact Lisa Starr, Senior Manager of Program Oversight, at (202) 283-3607.

Attachment

Attachment

Draft Audit Report - Automated Monitoring is Needed on Virtual Infrastructure to Ensure Secure Configurations (Audit # 201320004)

RECOMMENDATION #1: Implement an automated management tool to ensure that host and vCenter settings remain in compliance with configuration standards.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation and will procure and/or develop an automated tool, or adapt existing monitoring infrastructure, to report Virtual Server Host Compliance.

IMPLEMENTATION DATE: 01/25/2016

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: Applies patches to hosts timely in accordance with IRS policy.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation and will apply patches to hosts timely in accordance with IRS policy.

IMPLEMENTATION DATE: 07/25/2014

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 #3: Implement audit log collection and review on hosts and vCenters in accordance with IRS policy, including logging when users access these devices, the logon and logoff times, and the activities conducted during access.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation and currently has an interim process in place to collect vCenter and ESXi 5 virtual host log files. IRS Cybersecurity will develop an Audit Plan and implement virtual log file collection and review for both the vCenter and virtual infrastructure host servers.

Attachment

Draft Audit Report - Automated Monitoring is Needed on Virtual Infrastructure to Ensure Secure Configurations (Audit # 201320004)

IMPLEMENTATION DATE: **01/25/2015**

RESPONSIBLE OFFICIAL: 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.