



*An Enterprise Approach Is Needed
to Address the Security Risk
of Unpatched Computers*

September 25, 2012

Reference Number: 2012-20-112

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(f) = Risk Circumvention of Agency Regulation or Statute

Phone Number | 202-622-6500

E-mail Address | TIGTACommunications@tigta.treas.gov

Website | <http://www.tigta.gov>



HIGHLIGHTS

AN ENTERPRISE APPROACH IS NEEDED TO ADDRESS THE SECURITY RISK OF UNPATCHED COMPUTERS

Highlights

**Final Report issued on
September 25, 2012**

Highlights of Reference Number: 2012-20-112
to the Internal Revenue Service Chief
Technology Officer.

IMPACT ON TAXPAYERS

Patch management is an important element in mitigating the security risks associated with known vulnerabilities. The IRS has taken some actions to address patch management weaknesses, but an enterprise approach is needed to fully implement and enforce patch management policy. Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over the vulnerable computers and get access to the sensitive data they may contain, including taxpayer data.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the effectiveness of the IRS security patch management process. The implementation of effective patch management processes has been an ongoing challenge for the IRS, with patch issues reported in numerous prior TIGTA and Government Accountability Office reports. This audit is included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

Although progress has been made to automate installation and monitoring of patching in a large segment of its Windows environment, the IRS has not yet implemented key patch management policies and procedures needed to ensure all IRS systems are patched timely and operating securely. Specifically, the IRS has not completed implementation of an accurate and

complete inventory of its information technology assets, which is critical for ensuring that patches are identified and applied timely for all types of operating systems and software used within its environment.

In addition, the IRS needs to improve patch policy and monitoring processes to ensure patches are applied timely. The IRS also has not implemented controls to ensure that unsupported operating systems are not putting the IRS at risk. The IRS needs enterprise-level oversight and leadership to complete the implementation of its standardized patch management program and to achieve the benefits of implementing enterprise-wide patching solutions.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS implement enterprise-level responsibility to set and enforce IRS patch management policy, complete deployment of an automated asset discovery tool and build an accurate and complete inventory of information technology assets, take an enterprise-wide approach to buying tools to avoid redundancy and excessive cost, and complete implementation of controls to ensure that unsupported operating systems are not putting the IRS at risk.

The IRS agreed with TIGTA's recommendations and planned appropriate corrective actions for seven of the eight recommendations. Although the IRS agreed with the intent of the recommendation to hold system owners accountable for patching computers within prescribed time frames, it stated that its existing procedures addressed this recommendation and planned no corrective actions. While TIGTA believes further actions could have been taken, TIGTA also believes the IRS will address this issue through other planned corrective actions to update its patch management policy to provide clear standards for patch installation and to assign the responsibility to the Cybersecurity organization for ensuring enterprise-wide compliance with patch management policies.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 25, 2012

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael E. McKenney

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

SUBJECT: Final Audit Report – An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers (Audit # 201220006)

This report presents the results of our review to evaluate the effectiveness of the Internal Revenue Service security patch management process. This review is part of the Treasury Inspector General for Tax Administration's Fiscal Year 2012 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 XI.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Table of Contents

BackgroundPage 1

Results of ReviewPage 4

 Some Actions Have Been Taken to Address Patch
 Management Weaknesses, but an Enterprise Approach
 Is Needed to Fully Implement and Enforce Patch
 Management PolicyPage 4

 An Automated Means to Control an Inventory of
 Information Technology Assets Has Not Been Fully
 ImplementedPage 6

Recommendation 1:.....Page 8

Recommendation 2:.....Page 9

 Patch Policy and Monitoring Processes Need
 Improvement to Ensure Patches Are Installed TimelyPage 9

Recommendations 3 through 6:.....Page 14

Recommendation 7:.....Page 15

 Outdated and Unsupported Operating Systems on the
 Network Cannot Be Patched to Correct Known
 Vulnerabilities.....Page 15

Recommendation 8:.....Page 16

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 18

 Appendix II – Major Contributors to This Report.....Page 20

 Appendix III – Report Distribution ListPage 21

 Appendix IV – *****2(f)*****
 *****2(f)*****Page 22



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix V – *****2(f)*****
*****2(f)*****Page 23

Appendix VI – Associate Chief Information Officer Monthly
Critical Patch Report Patch Bulletin Tracking From Release DatePage 24

Appendix VII – Associate Chief Information Officer Monthly
Critical Patch Report Age AnalysisPage 25

Appendix VIII – *****2(f)*****Page 26

Appendix IX – Prior Treasury Inspector General for Tax
Administration Audit Reports With Security Patch Management
Issues.....Page 27

Appendix X – Glossary of TermsPage 30

Appendix XI – Management’s Response to the Draft ReportPage 34



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Abbreviations

ACIO	Associate Chief Information Officer
BDNA	Business DNA
CSIRC	Computer Security Incident Response Center
DDMA	Discovery and Dependency Mapping Advanced
EOps	Enterprise Operations
EUES	End User Equipment and Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
KISAM	Knowledge Incident/Problem Service Asset Management
MITS	Modernization and Technology Services
TIGTA	Treasury Inspector General for Tax Administration



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Background

Patch¹ management refers to the process by which an organization installs patches, which are fixes or updates to computer programs, operating systems, or applications. From a security perspective, patch management is an important element in mitigating the security risks associated with known vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a security patch or work-around to mitigate the vulnerability. Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gain control over the vulnerable machines, and get access to the sensitive data contained on the computer, destroy information on the computer, or use the computer as a launching point for additional attacks to other computers on the network. In addition, outdated and unsupported software is more vulnerable to attack and exploitation because vendors no longer provide updates, including security updates.

Ninety percent of successful attacks occurred against previously known vulnerabilities where a patch or secure configuration standard was already available.

The vast majority of vulnerabilities exploited by malicious code are ones for which a fix is available from the software vendor. A recent Gartner report stated that “ninety percent of successful attacks occurred against previously known vulnerabilities where a patch or secure configuration standard was already available.”² The Department of Defense lists the patching of operating systems and applications as the number one and number two priorities of its top 35 strategies³ to mitigate cyber intrusions.

The Internal Revenue Service (IRS) has more than 100,000 computers comprised of various operating systems and software that the IRS must ensure receive timely installation of security patches. Various organizations within the IRS manage their own computers and patching processes. Most have developed standard operating procedures for patching the various types of operating systems they manage.

Within the IRS, the patch management process generally consists of four segments: 1) identification and notification, 2) testing, 3) installation, and 4) monitoring and follow-up. The Computer Security Incident Response Center (CSIRC) within the Cybersecurity organization has primary responsibility for identifying and notifying the various IRS business

¹ See Appendix X for a glossary of terms.

² Terrance Cosgrove, Gartner, *Managing the Next Generation of Client Computing* (Feb. 8, 2011).

³ Department of Defense, Intelligence and Security, *Strategies to Mitigate Targeted Cyber Intrusions* (originally published Feb. 18, 2010; last updated July 18, 2011).



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

organizations about hardware and software vulnerabilities and patch availability. Once vendor-provided vulnerability notifications are received, the CSIRC performs technical evaluations based on enterprise metrics and rates the severity of the notifications. Internal patch advisories are then published and disseminated to technical points of contact throughout the IRS. Upon receipt of CSIRC advisories, points of contacts or system administrators within the various business organizations conduct patch testing, installation, monitoring, and follow-up for their various types of computer operating systems and software.

The implementation of effective patch management processes has been an ongoing challenge for the IRS. The Treasury Inspector General for Tax Administration (TIGTA) has issued numerous reports containing findings relating to patch management.⁴ From an overview perspective, these reviews found that the IRS had made commendable progress towards improving patch identification, testing, and monitoring processes. However, controls over patch installation continued to allow unpatched systems. The patches were not always installed for two primary reasons: 1) the automated approach used to install patches on Windows[®]-based⁵ systems did not always have valid connections to the systems requiring patching, and 2) system administrators did not always install patches due to the impact they believed such patches would have on systems under their control or due to the labor-intensive process of manually installing patches on numerous systems.

Also, the Government Accountability Office has issued several reports with findings related to IRS patch management activities; the latest was issued in March 2012.⁶ The Government Accountability Office reported that the IRS did not always apply critical patches or apply them in a timely manner and allowed the use of unsupported software for which the vendor no longer provides updates. Running outdated and unsupported operating systems increases the risk that known vulnerabilities will be exploited because the vendor will no longer be supplying any security patches for these systems. Operating systems in use at the IRS that were affected by these findings included UNIX, Windows, Oracle databases, and network devices.

In 1997, the IRS identified computer security as a material weakness under the Federal Managers' Financial Integrity Act of 1982.⁷ The Act requires that each agency conduct annual evaluations of its systems of internal accounting and administrative controls and submit an annual assurance statement on the status of the agency's system of management controls. As part of the evaluations, agency managers identify control areas that can be considered material

⁴ See Appendix IX for a list of reports.

⁵ Windows is a registered trademark owned by Microsoft Corporation.

⁶ Government Accountability Office, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).

⁷ Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

weaknesses.⁸ The IRS identified configuration management, of which patch management is a component, as one of its nine subsections of its computer security material weakness⁹ because it had not effectively implemented configuration management and change controls to safeguard the security and integrity of IRS systems.

The IRS has tasked the Enterprise Services organization with resolving its material weakness in configuration management. To accomplish effective configuration and change management, standard baseline configurations for all IRS assets must be documented, and then all changes to these baseline configurations must be tracked, including changes due to patching. The Enterprise Services organization is in the process of implementing the Enterprise Configuration Management System to assist the enterprise in effectively monitoring and enforcing configuration and change management. The first release of the Enterprise Configuration Management System was deployed at the end of July 2012.

This review was performed in the office of the IRS Information Technology (IT)¹⁰ organization in New Carrollton, Maryland, during the period September 2011 through July 2012. 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.

⁸ The Department of the Treasury has defined a material weakness as “shortcomings in operations or systems which, among other things, severely impair or threaten the organization’s ability to accomplish its mission or to prepare timely, accurate financial statements or reports.”

⁹ The nine subsections of the computer security material weakness are (1) network access controls, (2) system and application access controls, (3) system software configuration, (4) security roles and responsibilities, (5) separation of duties, (6) contingency planning, (7) audit trails, (8) security-related training, and (9) certification and accreditation. The IRS has completed actions to remediate the separation of duties, training, and certification and accreditation subsections.

¹⁰ On July 1, 2012, the Modernization and Information Technology Services (MITS) organization changed its name to IRS Information Technology.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Results of Review

The IRS has taken actions to improve its patch management processes and is in the process of implementing enterprise solutions to automate control of its information technology asset inventory and to address configuration and patch management weaknesses. The IRS has established patch management policy, yet key elements have not been implemented, and patch installation practices continue to result in unpatched or untimely patched computers. Further, the IRS has not implemented controls to address outdated and unsupported operating systems in its environment. Vendors for these operating systems no longer issue patches for these systems, which increases the risk that known security vulnerabilities may be exploited. IRS officials stated that until the IRS's change and patch management enterprise solution is implemented, the IRS will continue to lack the capability to effectively monitor and enforce patch management.

Some Actions Have Been Taken to Address Patch Management Weaknesses, but an Enterprise Approach Is Needed to Fully Implement and Enforce Patch Management Policy

The IRS has established Internal Revenue Manual (IRM) 10.8.50, *Information Technology Security, Service-wide Security Patch Management*, that provides policies and guidance to be used by IRS organizations to carry out their respective responsibilities in information systems security regarding security patch management. This policy incorporates guidance from the National Institute of Standards and Technology Special Publication 800-40, *Creating a Patch and Vulnerability Management Program*, Treasury Directive Policy 85-01, *Department of Treasury Information Technology Security Program*, and industry best practices.

In March 2008, the IRS assigned the Enterprise Operations (EOps) organization the responsibility to implement a standardized Patch Management process by April 1, 2008, in order to address TIGTA and Government Accountability Office repeat findings that servers were not patched or not timely patched or were noncompliant because of unsupported versions of software. The Infrastructure Executive Steering Committee recommended the use of the following tools for patch management on IRS servers: N1 for UNIX operating systems, Oracle Enterprise Manager for Oracle databases, and Altiris for Windows operating systems. The role of the EOps organization was to implement the Patch Management process within the EOps organization and to provide guidance to other business organizations within the IRS. In April 2008, the EOps organization completed implementation of Altiris 6.9 as its standardized automated patch management tool for Windows servers. All IRS server owners were expected to follow this process by June 30, 2008.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

In November 2008, the End User Equipment and Services (EUES)¹¹ organization began deployment of Altiris 6.9 for workstations. Altiris is designed to automatically install only required patches on workstations. It eliminates the manual database querying that was required repeatedly with Tivoli^{®12} during the software distribution cycle to determine target systems. Altiris uses “pull” technology, unlike other solutions, including Tivoli. For workstations, pull technology allows client computers, no matter how long they have been disconnected from the network, to download policies and tasks that apply to them as soon as they reconnect. As such, there is no “distribution window” that can be missed by client computers not online during that time period. Rather, the patch is always in a state of deployment until superseded or otherwise retired. In other words, simply connecting a workstation to the network results in automatic patch installation, and no manual patch installations by support personnel are needed.

Windows servers and workstations that have the Altiris software installed periodically communicate to Altiris notification servers from which the IRS posts patching compliance rates on dashboards or prepares other monitoring reports. System administrators have the opportunity to monitor patch installation on the Altiris dashboards, follow up on any failed patch statuses, and reconcile any information reported on the dashboard that appears incorrect.

Although progress has been made to automate installation and monitoring of patching in a large segment of its Windows environment, the IRS was unable to implement the EOps organization standardized patch management process enterprise-wide. Currently, a number of IRS organizations manage their own patch management process for their operating systems and applications using a variety of tools, as indicated in Appendix IV. The IRS relies on each of these organizations to maintain and manually report the inventory of information technology assets they manage and the patch compliance rates for those assets.

In addition, the IRS informed us that patching is still manual for the majority of its UNIX operating systems and is not in accordance with IRM required patch frequencies. The IRS informed us that funding issues stopped the deployment of the N1 tool that was recommended by the Infrastructure Executive Steering Committee in March 2008 for automating UNIX operating systems. The EOps organization is currently testing a process for automating patching on its UNIX servers.

In order to complete the implementation of its standardized patch management program and to achieve the benefits of implementing enterprise-wide patching solutions, the IRS needs to implement enterprise-level oversight of its patch management program. A centralized approach, using enterprise-wide solutions, would save money by eliminating duplication of efforts. For example, multiple system administrators may be testing the same patch on similar computers. In

¹¹ On April 22, 2012, the EUES organization changed its name to the User and Network Services organization.

¹² Prior to Altiris, the IRS used the Tivoli application to deliver the most current versions of software and security patches to employees’ computers and to scan the network for maintaining computer inventory records. Tivoli is a registered trademark owned by International Business Machines.



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

addition, the IRS could save money by having enterprise-level oversight of the purchase and maintenance of automatic patch management tools for enterprise-wide use.

Due to the lack of enterprise-level oversight and leadership, the IRS has not yet implemented key elements of its patch management policies and procedures that are needed to ensure all IRS systems are patched timely and operating securely. Specifically, the IRS has not:

- Completed the implementation of an accurate and complete inventory of its information technology assets, which is critical for ensuring that patches are identified and applied timely for all types of operating systems and software used within its environment.
- Implemented patch policy and monitoring processes to ensure patches are applied timely enterprise-wide.
- Implemented controls to ensure that unsupported operating systems are not putting the IRS at risk.

An Automated Means to Control an Inventory of Information Technology Assets Has Not Been Fully Implemented

The IRM 10.8.50 requires the IRS to inventory its information technology assets to determine which hardware equipment, operating systems, and software applications are used within the organization. At a minimum, the inventory must contain operating systems, versions of all software, patch levels, and installed applications. The inventory must be updated in a timely manner as software is added or deleted from the baseline. Having an accurate and complete inventory is necessary to ensure all IRS information technology assets receive timely security patches for protection against known vulnerabilities. Industry best practices prescribe that organizations deploy an automated asset discovery tool to build an accurate and complete inventory of information technology assets that reside on their networks. The automated tool should record the type of software installed on each asset, including its version number and patch level.

The IRS has not fully implemented an automated means to control its inventory of information technology assets and has not built a complete information technology asset inventory of all systems connected to its network that includes data elements such as the type of operating system, patch level, system owner, and physical location of the asset. The IRS has not yet discovered all the information technology assets residing on its network, and, therefore, cannot ensure all information technology assets are appropriately patched. The IRS is in the process of implementing two automated asset discovery tools: 1) the Business DNA (BDNA) tool for establishing and validating an accurate and complete inventory of information technology devices on the IRS network, and 2) the Discovery and Dependency Mapping Advanced (DDMA)



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

tool for establishing an inventory of configuration items for which changes to configuration settings need to be managed, including changes due to patching.

- **BDNA.** The IRS Security Risk Management's Penetration Test and Code Analysis organization began implementation of the BDNA tool in October 2010. The data retrieved through BDNA network scans are maintained in a database. When fully implemented, the database will contain detailed information about each asset it identifies on the network, such as machine name, network address, operating system, installed software, and patches. The IRS is currently conducting scans of a partial segment of the IRS network and providing this data to the CyberScope. The IRS stated that the full implementation of the BDNA tool has been delayed due to technical issues, lack of resources, difficulties with gaining permission to scan all IRS networks, and higher IRS priorities such as the implementation of the Customer Account Data Engine 2 and systems related to complying with the new healthcare laws.

In its limited initial scanning, the BDNA tool identified 1,238 Windows servers on the IRS network, as of March 2012, that were not in the IRS's official inventory, which is the Knowledge Incident/Problem Service Asset Management (KISAM).¹³

The BDNA staff expects to complete implementation of BDNA by September 2012, with the capability to scan the entire IRS network four times a month. Eventually, the IRS plans to provide BDNA data to system owners so they can reconcile and validate the data that was placed in the KISAM from the Information Technology Asset Management System, the IRS's previous asset inventory system.

- **DDMA.** In addition, the IRS Enterprise Services Configuration and Change Management organization is in the process of implementing the Enterprise Configuration Management System for the purpose of implementing effective configuration and change management and resolving the IRS's computer security material weakness in configuration management. To accomplish effective configuration and change management, standard baseline configurations for all IRS assets need to be documented as well as all configuration changes tracked, including changes due to patching. To establish this inventory, the Enterprise Services organization is in the process of deploying the DDMA tool, an automated asset discovery tool similar to the BDNA tool, but for the purposes of establishing an inventory of configuration items for which changes to configuration settings need to be managed.

The data gathered by the DDMA asset discovery tool will be maintained in a database, where the Enterprise Services organization will track authorized and unauthorized changes to IRS assets. The first release of the Enterprise Configuration Management

¹³ KISAM was deployed in September 2011 and replaced the Information Technology Asset Management System, the IRS's previous asset inventory system.



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

System is scheduled to be deployed the end of July 2012, and the DDMA tool will first begin collecting data on computers in the IT organization-owned test environments prior to expanding to the IRS production environment. The Enterprise Services organization stated that until the Enterprise Configuration Management System is implemented, the IRS will continue to lack the capability to effectively implement configuration and change management.

The National Institute of Standards and Technology recommends that patch management and vulnerability scanning capabilities be integrated within one agent instead of having to install and manage two separate agents on each computer. Because it is costly from an information technology management point of view to install and manage multiple agents on each computer, it would be ideal if both functions (patching and inventorying) could be performed by the same product.

While both the BDNA and the DDMA databases will contain essential data for monitoring patching compliance, the IRS does not have an approach for making use of the data collected by these tools to support its patch management program.

Although IRS policy requires the IRS to establish an enterprise-level group with responsibility for patch management, no enterprise-level group exists to coordinate or address comprehensive approaches to enterprise patching solutions. In addition, the IRS's decentralized management environment and multiple networks have slowed implementation of enterprise-wide tools.

Without proper knowledge or control of the hardware and software in its environment, the IRS cannot effectively manage patches in order to properly secure its information technology assets.

Recommendations

The Chief Technology Officer should ensure that the IRS:

Recommendation 1: Completes the deployment of an automated asset discovery tool (or tools, if needed) and builds an accurate and complete inventory of information technology assets (including hardware and software) that reside on the IRS network.

Management's Response: The IRS agreed with this recommendation. BDNA is an automated asset discovery tool for non-mainframe networked systems. The IRS will complete the BDNA deployment by October 2012. Once deployed, enterprise assets will be provisioned with BDNA credentials, and BDNA will assist in building an accurate and complete hardware and software inventory for the KISAM system. BDNA will provide data in accordance with the National Institute of Standards and Technology Special Publication 800-40, Section 2.2.1, that addresses information technology inventory for network port, software configuration, and hardware configuration.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Recommendation 2: Takes an enterprise-wide approach to buying tools to avoid redundancy and excessive cost, and develops an approach for using the data collected by its enterprise tools to support its patch management program, including data collected by the BDNA tool and the DDMA tool.

Management's Response: The IRS agreed with this recommendation. With respect to the first part of this recommendation relating to the enterprise-wide purchase of tools, the Enterprise Services organization ensures that products are selected based on enterprise solutions through the IT Configuration Control Board. Tools are, and shall continue to be, analyzed for redundant and duplicate features. Where possible, redundant tools will be eliminated before new tools are approved for use. Where duplication or redundancy is required to provide defense in depth or breadth, this need will be reflected in the usage guidance in the tools record within the Enterprise Standards Profile. The Change Request process, subservient to the IT Configuration Control Board process, ensures that an engineering analysis of tools is conducted to avoid redundancy and excessive cost. This is a current and ongoing process. Therefore, the IRS considers this part of the corrective action to be closed.

With respect to the second part of this recommendation relating to the development of an approach for using the data collected by enterprise tools to support patch management, the Enterprise Services, Cybersecurity, and EOps organizations will develop an approach to utilize the data from various sources to ensure that the patch management program is efficient and effective. This approach will include the collection of data, analysis of patching requirements, and preparing an implementation plan.

Patch Policy and Monitoring Processes Need Improvement to Ensure Patches Are Installed Timely

Critical patches continue to be missing or are installed in an untimely manner

The IRM 10.8.50 requires timely implementation of security patches on all IRS systems and monitoring to ensure systems are patched as required. The IRS relies on a number of patch management tools and the reports generated from these tools to monitor patch compliance for a majority of its computer systems. However, the IRS's own patch monitoring reports continue to report unpatched or untimely patched computers. For example:

- An IRS-wide patch monitoring report for Windows servers, called the Associate Chief Information Officer (ACIO) Monthly Critical Patch Report, showed the IRS's overall patch compliance rate¹⁴ for critical patches averaged 88 percent in March 2012, ranging

¹⁴ The patch compliance rate is the number of patches applied to servers divided by the number of applicable patches for servers.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

from a low of 63 percent to a high of 88 percent for the six-month period October 2011 to March 2012 (see Appendix V, which shows IRS patch compliance is inconsistent across the board). The March 2012 report showed that 7,329 potential vulnerabilities remain on IRS servers because 23 critical patches had not been installed on servers that need them, some released as far back as April 2011 (see Appendix VI). These vulnerabilities could potentially be exploited to gain unauthorized access to information, disrupt operations, or launch attacks against other systems.

- The CSIRC organization publishes the list of critical and high patches and their installation statistics in its Cyber Daily Report¹⁵ as reported by the IRS organizations that are responsible for patching their own systems. The Cyber Daily Reports for January, February, and March 30, 2012, showed that critical and high-risk patches the CSIRC had issued on October 11 and November 8, 2011, were still outstanding.
- For EOps-managed Windows servers using the Altiris patching tool, the Altiris Patch Dashboards for the period October 2011 to March 2012 showed that the EOps organizations' overall patch compliance rate for that time period averaged 87 percent, ranging from as low as an average of 44.41 percent to as high as 99.57 percent compliant (see Appendix VIII). While higher patch compliance rates are desirable, organizations with higher patch compliance rates also often have a number of missing patches. For example, an organization with an overall patch compliance rate of 90.97 percent in March 2012 had at least one or more missing patches for 68 (47 percent) of its total 145 servers.

In addition to missing patches, we found the IRS is not timely patching its computers. The IRS informed us that it expects critical patches to be installed within 72 hours. Our review of the ACIO Monthly Critical Patch Reports for the months of January, February, and March 2012 showed the IRS continues to patch servers in an untimely manner (see Appendix VII). During this time period, it took an average of 55 days to install critical patches, ranging from three to 114 days.

The IRS organizations cited various reasons for not installing critical patches on its servers, including:

- Deployment approval under moratorium must be obtained.
- Server upgrade or regularly scheduled maintenance was pending.

¹⁵ Because not all IRS business organizations report patch data to the CSIRC for inclusion in the Cyber Daily Report, the IRS indicated that this report is considered informational only to provide situational awareness of the overall security posture of the enterprise and not official reportable numbers or measures. For example, the Cyber Daily Report did not include patch results for the Integrated Submission and Remittance Processing; the Research, Analysis, and Statistics; and the Statistics of Income organizations and the Small Business/Self-Employed and Wage and Investment Divisions.



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

- Patch caused issues and roll-back was needed.

Examples of the missing critical patches reported on the March 2012 ACIO Monthly Critical Patch Report included:

- *****2(f)*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****
- *****2(f)*****
 *****2(f)*****
 *****¹⁶ *****2(f)*****
 *****2(f)¹⁷*****
 *****2(f)*****.
- *****2(f)*****
 *****2(f)¹⁸*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****.

Patch management policy does not provide clear expectations for when patches must be installed. IRM 10.8.50 specifies that distribution of critical patches must begin within 72 hours of patch availability and high patches within five business days. However, it does not specify an expectation for when that critical or high patch must be installed on vulnerable assets.

In addition, the IRS has no mechanism to enforce timely patching or to hold system owners accountable for ensuring their systems are timely patched or to ensure system owners formally accept the risk of not patching systems timely. By not installing security patches in a timely fashion, the IRS increases the risk that known vulnerabilities in its systems may be exploited.

¹⁶ *****2(f)*****.

¹⁷ *****2(f)*****
 *****2(f)*****
 *****2(f)*****
 *****2(f)*****.

¹⁸ *****2(f)*****.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Monitoring of patch installation needs improvement

IRS processes to monitor the installation of required patches need improvement. The IRS's current monitoring processes are not sufficient to ensure that vulnerabilities resulting from unpatched systems are successfully and timely remediated. The IRS depends on the various IRS organizations that manage their own computers to frequently self-report patching data from their organization-level patch monitoring reports. This effort is labor intensive and results in incomplete and unverified patch data. In addition, the IRS informed us that the Altiris enterprise patch management tool¹⁹ currently in use did not always provide accurate patch compliance data, and that its reporting module needed improvement.

Server patch reporting is managed by the EOps organization and is reported via the ACIO Monthly Critical Patch Report. As the title indicates, this report is specific to the patches defined as critical. The EOps organization extracts data for EOps-managed servers through the Altiris tool and relies on manual business organization input for patch data related to servers not managed by the EOps organization.

Workstation patch reporting for the majority of EUES-managed workstations is reported through the Altiris Patch Dashboard managed by the Enterprise System Management organization and housed in the Enterprise Systems Management-Online data store. Workstation patch reporting for non-EUES-managed workstations is by manual self-reporting from the owning business organizations.

Data from these two primary sources are used by the Cybersecurity organization to produce summary patch measures that are reported on the IT organization's IT Internal Dashboard. The IT Internal Dashboard scores various measures as red, yellow, or green as a summary of notable trends for IRS executives. The scorecard includes as a measure the percentage of critical patches installed. The critical patch measure was red in January, February, and March 2012 for non-IT²⁰-managed computers due to lack of input of their patch data. For example, in March 2012, the IT organization reported that it had not received for 14 consecutive months percentage data from non-IT-managed Windows workstations needing critical patches, which it needed to track patch metrics in its IT Internal Dashboard.

Further, while the Altiris tool automates patching installation and monitoring for Windows-based computers, the IRS informed us that the Altiris patch management tool version 6.9 did not always provide accurate patch status data and that its reporting module needed improvement. For example, for several months beginning in January 2012, EOps

¹⁹ Enterprise patch management tools scan for vulnerabilities on computers participating in this patching solution, provide information regarding needed patches and other software updates on those computers, and allow an administrator to decide on the patch process.

²⁰ The IT organization includes EOps and EUES. Non-IT organizations include Chief Counsel; Criminal Investigations; Integrated Submissions and Remittance Processing; the Office of Research, Analysis, and Statistics; Statistic of Income; and the Small Business/Self-Employed Division and the Wage and Investment Division.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

organization staff had stopped sending Altiris missing patch reports for Windows servers to system administrators due to the inaccuracies in the reports. Five EOps suborganizations with consistently low overall patch compliance rates informed us that their low scores were due to 1) not applying patches, 2) lack of resources to apply missing patches, 3) the Altiris software not working properly, 4) incorrect Altiris collection policy settings, or 5) retired servers that should be removed from the dashboard. However, these EOps suborganizations were not reviewing the Altiris Patch Dashboard to verify patching compliance due to its inaccuracies and lack of sufficient detail to determine causes for why a patch may not have been installed.

In addition, we found that not all EOps-managed Windows servers were being monitored by the Altiris tool. For example, we identified 85 EOps-managed Windows servers in the IRS production environment that in February 2012

*****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****

The EOps organization staff indicated that they were uncertain why these servers were not on the dashboard, but that it may be due to either the Altiris software not working properly or never having been installed. The Altiris reporting module does not provide sufficient detail to indicate why failures occurred, does not alert system administrators when the Altiris patching software is not working properly, and does not maintain historical data from month to month.

EOps organization officials also indicated that these servers may not have appeared on the Altiris Patch Dashboard because they were not defined in the KISAM database as “in use.” The IRS is working to resolve this deficiency and other transition issues that occurred when migrating servers from a prior database to KISAM. For example, in March 2012, there were 965 Windows servers listed in the Altiris Patch Dashboard as “unknown responsibility,” due to transition issues (*i.e.*, the IRS has not determined who the system owners are).

Likewise, the EUES organization was having patch reporting discrepancies for workstations. The IRS is in the process of upgrading Altiris 6.9 to Altiris 7.1²¹ for its Windows-based computers. However, the IRS has encountered a number of infrastructure issues in its transition to Altiris 7.1. For example, due to the Altiris 7.1 infrastructure not being stable in the EUES organization workstation environment, the Enterprise System Management Patch Management website was not accurate in March 2012 and was able to report on only 88 percent of the enterprise. No data existed for the remaining 12 percent. The IRS expects to resolve the infrastructure issues and deploy Altiris 7.1 by the end of Calendar Year 2012.

²¹ Symantec purchased the Altiris software on April 6, 2007.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

We found no enterprise-level group enforcing IRS policy to implement effective automated patching and monitoring processes to ensure patches are installed timely. Also, ineffective automated reporting increases burden on IRS resources to manually validate patch statuses. If patch monitoring is inadequate, the IRS has no assurance that patches are applied timely and IRS assets are secure.

Recommendations

The Chief Technology Officer should:

Recommendation 3: Update patch management policy to provide clear expectations for when patches must be installed based on criticality.

Management's Response: The IRS agreed with this recommendation. The IRS will update the patch management policy in the IRM 10.8.50, providing clear standards for timeliness of patch installation based on criticality.

Recommendation 4: Implement procedures to hold system owners accountable for patching computers within prescribed time periods.

Management's Response: The IRS agreed with the spirit and intent of the recommendation. The IRS believes that their existing procedures address this recommendation.

Office of Audit Comment: Although the IRS's existing procedures require system owners to be responsible for patching their systems in a timely manner, the results of our review revealed that the IRS needs to improve enforcement of its patch policy. In addition, the existing policy does not provide clear expectations for when patches must be installed based on criticality. However, we believe this issue will be addressed by the IRS's planned corrective actions to update its patch management policy to provide clear standards for patch installation and to assign the responsibility to the Cybersecurity organization for ensuring enterprise-wide compliance with patch management policies.

Recommendation 5: Establish patch performance metrics in terms of setting compliance rate goals and measure them on a monthly basis.

Management's Response: The IRS agreed with the spirit and intent of this recommendation. The IRS will update the patch performance metric policy in IRM 10.8.50, providing clear standards for timeliness of patch installation based on a risk assessment of criticality. The IRS will collect patch performance metrics and establish a periodic monitoring process.

Recommendation 6: Implement enterprise-level responsibility to set and enforce IRS patch management policy, to include deployment of enterprise patch management tools that automate patch installation and monitoring for like operating systems and software.



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

Management's Response: The IRS agreed with this recommendation. The IRS will update the patch management policy in IRM 10.8.50 to set patch management standards. The Cybersecurity organization will have responsibility for ensuring enterprise-wide compliance with patch management policies. Cybersecurity will partner with other organizations within the IRS IT organization as well as with other IRS business and operating divisions to accomplish this corrective action.

Recommendation 7: Correct the issues with Altiris patch management tool reporting capabilities.

Management's Response: The IRS agreed with this recommendation. Currently, the reporting module of the IRS enterprise patching solution (Altiris) does not support the consolidation of information across their patching nodes. To address this recommendation, the IRS will engage the Altiris vendor to develop an enterprise-level reporting capability. In the interim, the IRS has taken steps to extract the data from multiple nodes and collect it in a repository to facilitate the presentation of an enterprise view.

Outdated and Unsupported Operating Systems on the Network Cannot Be Patched to Correct Known Vulnerabilities

IRS policy states that system administrators should ensure the version of the operating system being used is one for which the vendor still offers standardized technical support. This policy exists because one of the biggest network security risks is outdated systems that are no longer supported by their vendors. Older security flaws on these systems have been known for years and have likely been patched. However, newer security risks designed to exploit the more current version of the systems have a high probability of existing on these outdated systems. In other words, the risks lie not only with the previously known security risks but with new security risks for which these systems never received, and never will receive, an update or fix.

*****2(f)*****
*****2(f)*****

*****2(f)*****. However, the IRS could not locate or identify the owners responsible for the remaining 65 obsolete and unsupported servers. As a



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

result, the IRS did not know why these servers were still operational and connected to its network.

The IRS has not completed corrective actions for retiring obsolete technology in response to a prior TIGTA finding.²² The TIGTA recommended that the IRS Chief Technology Officer should ensure an enterprise-wide strategic plan was developed to address the outdated database version issues prevalent in the IRS production environment. The IRS agreed with the recommendation and stated that the IRS Enterprise Services organization would coordinate with the affected stakeholders to develop a strategic plan for obsolescence of technology to include database version control.

In August 2011, the Enterprise Services organization developed a plan for retiring obsolete technology entitled, *IRS Obsolete Technology Retirement Process*. However, the IRS is still in the beginning stages of implementing its plan. The plan cited the following internal impediments to remediating the obsolete technologies:

- Lack of systematic process to retire obsolete technologies.
- Lack of ownership of process and its components.
- Challenge facilitating coordination between multiple stakeholders.
- Dependencies of upgrades on other related products and applications.
- Time required to evolve replacement technologies.
- Complexity involved for testing all aspects of major upgrades in nonproduction environment.

Running outdated and unsupported operating systems increases security exposure because the vendor will not be supplying any security patches for any security vulnerabilities arising since the products' end of life. *****2(f)*****
*****2(f)*****
*****2(f)*****
*****2(f)*****. Therefore, this vulnerability remains an inherent part of that operating system.

Recommendation

Recommendation 8: The Chief Technology Officer should complete implementation of controls to ensure that unsupported operating systems are not putting the IRS at risk.

²² TIGTA, Ref. No. 2011-20-044, *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (May 2011).



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Management's Response: The IRS agreed with this recommendation. The Enterprise Services organization will ensure that only supported operating systems are in use at the IRS through the use and monitoring of the Universal Configuration Management Database. Unsupported operating systems will be identified, the owners will be notified, and corrective actions will be taken to remove or replace the systems in order to prevent and reduce risks to IRS networks. The implementation due date of this corrective action is dependent on the successful deployment of the Universal Configuration Management Database, with a target completion date of July 1, 2013.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of the IRS security patch¹ management process. To accomplish the objective, we:

- I. Determined whether patch management policies and procedures have been established and implemented as recommended by the National Institute of Standards and Technology, the Department of the Treasury, and best practices.
 - A. Obtained and review policies, standards, and procedures on patch management.
 - B. Determined whether IRS management regularly analyzes patch reports to update patch management policies and procedures.
 - C. Reviewed the IRS's efforts to close the Computer Security Material Weakness as it relates to patch management.
- II. Determined how the IRS maintains an up-to-date information technology asset inventory for patch management.
 - A. Interviewed the EOps organization (and other organizations that maintain their own inventory) on the process used to maintain the information technology asset inventory list for applying patches.
 - B. Determined how inventory lists maintained through functionality of Altiris, Tivoli, and BNDNA software are associated with the KISAM (the authoritative inventory of information technology assets).
 - C. Determined whether the information technology assets inventories from the Altiris, Tivoli, and BNDNA tools are reconciled with KISAM and Active Directory records to identify discrepancies.
- III. Determined how the IRS ensures that all system components and software have the latest vendor-supplied security patches installed.
 - A. Interviewed management on the processes used to identify patch levels and missing patches.
 - B. Interviewed BNDNA, Tivoli, and Altiris subject matter experts on these tools' capabilities relating to patch management.

¹ See Appendix X for a glossary of terms.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

- C. Evaluated the IRS's monitoring process for patch levels and missing patches by reviewing patch exception reports.
- D. Reviewed missing patches from system scan reports and interviewed system owners and/or system administrators to determine the causes for low patch compliance rates.
- IV. Determined whether patches are applied timely to ensure protection of IRS computing components and information.
 - A. Interviewed IRS staff on timeliness criteria and reports used to monitor patch timeliness.
 - B. Reviewed patch monitoring reports to evaluate timeliness of patch installation and IRS follow-up efforts.
 - C. Interviewed system owners and/or system administrators to determine the causes for untimely patching.
- V. Determined the reasons why unsupported operating systems remain in use and the risks associated with their use.
 - A. Identified unsupported operating systems in use.
 - B. Determined reasons why unsupported operating systems remain in use.
 - C. Determined the risks associated with unsupported operating systems remaining in use.

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 policies, procedures, and practices for identifying, testing, installing, and monitoring security patches on IRS operating systems. We evaluated these controls by reviewing IRS policy and procedure documents, interviewing IRS personnel, reviewing IRS patch monitoring reports, performing our own testing for missing patches, and analyzing IRS reasons for missing patches.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

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

Charles Ekunwe, Senior Auditor

Cari Fogle, Senior Auditor

Bret Hunter, Senior Auditor

Esther Wilson, Senior Auditor

Elton Jewell, Information Technology Specialist



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Chief Counsel CC
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Director, Office of Research, Analysis and Statistics RAS
Chief, Criminal Investigation SE:CI
Director, Statistics of Income RAS:S
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
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



An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers

Appendix IV

*****2(f)*****

*****2(f)*****

*****2(f)*****	*2(f)*	**2(f)**	*****2(f)*****	****2(f)****	***2(f)***
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)*****	**2(f)**	**2(f)**
2(f)**	*2(f)*	**2(f)**	*****2(f)***** ¹	**2(f)**	**2(f)**

*****2(f)*****

¹ *****2(f)*****
*****2(f)*****
*****2(f)*****.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix VI

*Associate Chief Information Officer
Monthly Critical Patch Report Patch Bulletin
Tracking From Release Date*

ACIO Monthly Critical Patch Report Patch Bulletin Tracking From Release Date to March 2012						
Bulletin	Vendor Severity	Released Date	Compliance	Applicable	Installed	Vulnerable
2(f)	Critical	***2(f)***	78.30%	3,385	2,650	735
2(f)	Critical	***2(f)***	77.40%	2,103	1,627	476
2(f)	Critical	***2(f)***	61.70%	767	473	294
2(f)	Critical	***2(f)***	81.50%	3,424	2,792	632
2(f)	Critical	***2(f)***	84.70%	3,592	3,043	549
2(f)	Critical	***2(f)***	80.80%	3,567	2,881	686
2(f)	Critical	***2(f)***	46.40%	110	51	59
2(f)	Critical	***2(f)***	86.90%	3,557	3,092	465
2(f)	Important	***2(f)***	78.60%	771	577	194
2(f)	Critical	***2(f)***	74.80%	3,686	2,897	789
2(f)	Critical	***2(f)***	87.60%	3,613	3,164	449
2(f)	Critical	***2(f)***	30.00%	40	12	28
2(f)	Critical	***2(f)***	93.70%	3,676	3,443	233
2(f)	Critical	***2(f)***	82.90%	3,758	3,117	641
2(f)	Critical	***2(f)***	94.00%	3,409	3,204	205
2(f)	Critical	***2(f)***	95.50%	265	253	12
2(f)	Critical	***2(f)***	96.90%	3,020	2,927	93
2(f)	Critical	***2(f)***	95.30%	3,821	3,643	178
2(f)	Critical	***2(f)***	95.10%	3,821	3,633	188
2(f)	Critical	***2(f)***	95.60%	3,821	3,653	168
2(f)	Critical	***2(f)***	97.50%	3,042	2,966	76
2(f)	Critical	***2(f)***	97.50%	3,042	2,967	75
2(f)	Critical	***2(f)***	86.60%	779	675	104
Total Vulnerable						7,329

Source: ACIO Monthly Critical Patch Report for the month of March 2012. Total vulnerable represents the total number of flaws or weaknesses in IRS servers that could potentially be exploited to gain unauthorized access to information, disrupt operations, or launch attacks against other systems.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix VII

*Associate Chief Information Officer
Monthly Critical Patch Report Age Analysis*

ACIO Monthly Critical Patch Report Age Analysis – January, February, and March 2012							
Age	Servers	Business Organizations					
		CI	Counsel	ISRP	RAS	SB/SE	W&I
< 7 Days	1	0	1	0	0	0	0
7 > 30 Days	358	3	12	0	33	0	310
31 > 60 Days	1,744	108	487	1,085	60	4	0
61 > 90 Days	321	0	58	248	7	0	8
> 90 Days	85	0	4	0	15	0	66
Unable to Determine	733	103	530	0	0	3	97
Total	3,242	214	1,092	1,333	115	7	481

Source: ACIO Monthly Critical Patch Reports for the months January through March 2012. The days presented are based on the date when the business organization estimated the patch would be installed.

Legend: CI – Criminal Investigation; Counsel – Chief Counsel; ISRP – Integrated Submission and Remittance Processing; RAS – Research, Analysis, and Statistics; SB/SE – Small Business/Self-Employed; and W&I – Wage and Investment. Unable to Determine – Estimated patch installation date was not provided by the business organization.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix IX

Prior Treasury Inspector General for Tax Administration Audit Reports With Security Patch Management Issues

The following TIGTA audit reports contain patch¹ management issues.

1. TIGTA, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies* (Sept. 2011).

Issue: The Business Systems Modernization organization forest consisted of primarily Windows 2000 servers, which are outdated and no longer supported by the Microsoft Corporation. Patches are no longer issued for these servers, which remain a high security risk.

2. TIGTA, Ref. No. 2011-20-044, *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (May 2011).

Issue: Non-mainframe databases containing taxpayer data were not always configured in a secure manner and databases were running out-of-date software that no longer received security patches and other vendor support.

3. TIGTA, Ref. No. 2008-20-159, *Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network* (Aug. 2008).

Issue: The CSIRC vulnerability scan identified 2,093 authorized and unauthorized web servers with at least one high-, medium-, or low-risk security vulnerability. The scan report contained 540 web servers with at least one 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 when new vulnerabilities are identified.

4. TIGTA, Ref. No. 2008-20-029, *Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks* (Dec. 2007).

Issue: A majority of the IRS databases scanned do not have the latest software updates (patches) installed. TIGTA scans found that 65 percent of the databases scanned needed to be updated, with more than 300 databases being outdated from 11 to 20 months. As a result, outdated IRS databases were collectively susceptible to nearly 40,000 database

¹ See Appendix X for a glossary of terms.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

vulnerabilities, half of which are considered high risk. Also, installation of patches is not currently being monitored, and there is no automated tool available to detect whether patches have been installed.

5. TIGTA, Ref. No. 2006-20-167, *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk* (Sept. 2006).

Issue: TIGTA roll-up assessment of weaknesses with the IRS's software patching process found that controls over patch implementation continue to allow unpatched systems.

6. TIGTA, Ref. No. 2006-20-031, *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Feb. 2006).

Issue: Twenty-eight percent of the Windows workstations did not have the latest Common Operating Environment update installed, causing 16 missing security patches, six of which were deemed high risk by IRS standards.

7. TIGTA, Ref. No. 2006-20-021, *Progress Has Been Made on Using the Tivoli Software Suite, Though Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories* (Dec. 2005).

Issue: The IRS's use of the Tivoli Software Suite showed security patches were successfully installed only 67 percent of the time on Windows-based computers. Also, several security patch distributions had success rates below 50 percent, with some succeeding in as few as 18 percent of the instances.

8. TIGTA, Ref. No. 2005-20-143, *The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made* (Sept. 2005).

Issue: The CSIRC did not regularly perform follow-up activities to ensure critical patches are installed. Also, the CSIRC has been operating under draft patch management procedures since November 2003, which can hinder the CSIRC and system administrators in the IT organization in timely installing software patches on all appropriate computers. Lastly, problems identified during vulnerability scans and penetration tests were not formally provided to the business owners, and corrective actions were not documented in Plans of Action and Milestones as required by the Federal Information Security Management Act.² Unless requested by the business unit, the CSIRC did not always follow up to ensure corrective actions were implemented.

² Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

9. TIGTA, Ref. No. 2004-20-081, *Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented* (Mar. 2004).

Issue: Criminal Investigation management has not kept servers and workstations up to date with the latest security patches. The TIGTA identified 34 operating system vulnerabilities on the 32 computers tested that resulted because system administrators had not installed current security patches.

10. TIGTA, Ref. No. 2004-20-027, *Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses* (Jan. 2004).

Issue: The TIGTA's review of local servers and workstations at five locations identified significant security vulnerabilities. Vendor patches were not applied to hardware and software to ensure known vulnerabilities were adequately mitigated; 10 of 20 servers had at least one high-risk vulnerability that could have been resolved with current patches from the vendors. Also, managers did not actively monitor performance of five employees who were confused over who had responsibility for maintaining Windows workstations and servers as well as applying and testing computer patches.

11. TIGTA, Ref. No. 2003-20-118, *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (July 2003).

Issue: More than nine months had elapsed since the IRS enterprise internal firewalls had been patched. The operating system vendor had issued 51 recommended security patches during this time. The vendor of the external firewalls stopped supporting the installed version at least eight months before the TIGTA's review began.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix X

Glossary of Terms

Term	Definition
Advisories	The CSIRC communication for a patch.
Altiris	A patch assessment tool used by the IRS Enterprise Operations organization for Microsoft Windows servers and workstations.
Application	Any data entry, update, query, report, or program that processes data for the user.
Business DNA (BDNA (Discover))	BDNA (Discover) provides an in-depth view of all hardware and software deployed across an enterprise. BDNA (Discover) works without requiring software agents or administrative access, enabling it to be easily deployed across any size organization. BDNA (Discover) identifies hardware, software, and even IP-enabled, non-information technology devices.
Computer Security Incident Response Center	The IRS office that receives and disseminates incident information, responds to incidents, and reports on incidents.
Customer Account Data Engine 2	It is the next step in the IRS's information technology modernization efforts and it builds on the foundation of the Current Customer Account Data Engine. It is one of the IRS's top priority information technology investments. The Customer Account Data Engine 2 will provide faster refunds for millions of eligible individual taxpayers and faster payment postings, account updates, and taxpayer notices.
CyberScope	CyberScope was launched by the Office of Management and Budget on October 19, 2009, to provide for secure and efficient Federal Information Security Management Act ³ reporting by Federal agencies. Used to report a wide variety of information and complex metrics, it also provides meaningful analysis of agency security postures.

³ Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Term	Definition
Cybersecurity Organization	Assists all IRS divisions and functions in maintaining secure facilities, technology, and data by assuring the security and resilience of critical agency functions and business processes using risk-based decision-making practices.
Database	The term database or database management system refers to a collection of information organized in such a way that it can quickly select desired pieces of data. It uses a collection of programs to enter, organize, and select data.
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.
Discovery and Dependency Mapping Advanced (DDMA)	A component of the Enterprise Configuration Management System, it is a Hewlett-Packard tool that will do agentless discovery of assets on the network to establish the IRS inventory for configuration management. It can also report on patch levels.
Enterprise Configuration Management System	Provides a comprehensive enterprise-wide view of the IRS infrastructure including systems and applications; maintains the enterprise's configuration items accurately for configuration change management and the other information technology service management processes; and encompasses an integrated, automated, end-to-end configuration, change, and release management process.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Knowledge Incident/Problem Service Asset Management	Maintains the complete inventory of IT and non-IT organization assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the Enterprise Service Desk. The previous name for this system was the Information Technology Assets Management System.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Term	Definition
Malicious Code	Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.
MITS (now IRS IT)	Manages the IRS's enterprise-wide information resources and technology and is responsible for the IRS's long-range efforts for improving tax administration through modernized systems.
Moratorium	A restriction on changes to the IRS production environment during the 2012 Filing Season, <i>i.e.</i> , November 1, 2011, through May 21, 2012.
National Institute of Standards and Technology	Under the Department of Commerce, it is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Operating System	The master control program that runs a computer. It is 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.
Patch	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.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals that results from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Server	A physical computer dedicated to running one or more services as a host to serve the needs of users of other computers on the network.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
System Administrator	A person who manages the technical aspects of a system.
Tivoli	Tivoli endpoint is an agent-based product that can be configured to conduct port, network, and vulnerability scans.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Term	Definition
UNIX	An operating system well known for its relative hardware independence and portable application interfaces. Some of the popular UNIX derivatives are Linux, Solaris, HP-UX, and AIX.
Vulnerability (or Vulnerable)	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.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Appendix XI

Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

SEP 14 2012

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report—An Enterprise Approach Is Needed to
Address the Security Risk of Unpatched Computers
(Audit # 201220006) (e-trak # 2012-34847)

Thank you for the opportunity to review and respond to the subject audit report. Under separate memorandum, we are formerly requesting that the audit report be designated "Sensitive But Unclassified." In this correspondence, we are responding to report recommendations. We appreciate that your report acknowledged that the Internal Revenue Service (IRS) has established a patch management policy. We also thank you for reporting on the progress we made to automate installation and monitoring of patching in a large segment of our Windows environment.

The security and privacy of taxpayer information is of utmost importance to us, and your report recommendations will further assist us in mitigating security risks associated with patch management vulnerabilities. Of the eight report recommendations, we agree with six of them and agree with the spirit and intent of the remaining two report recommendations. For recommendation four, we believe our existing procedures address patching accountability. For recommendation five on patch performance metrics, we do not agree to the rigor of a structured compliance but we agree that a risk assessment is needed in which criticality is defined. The attachment to this memo details our planned corrective actions to implement the recommendations.

We value your continued support and the assistance and guidance your organization provides. If you have any questions, please contact me at (202) 622-6800 or David W. Stender, Associate Chief Information Officer for Cybersecurity, at (202) 622-8910.

Attachment



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Attachment

Draft Audit Report –An Enterprise Approach Is Needed to Address the Security Risk of Unprotected Patched Computers (Audit # 201220006 (e-trak # 2012-34847))

RECOMMENDATION #1: The Chief Technology Officer should ensure that the IRS completes the deployment of an automated asset discovery tool (or tools if needed) and builds an accurate and complete inventory of IT assets (including hardware and software) that reside on the IRS network.

CORRECTIVE ACTION #1: We agree with this recommendation. Business DNA (BDNA) is an automated asset discovery tool for non-mainframe networked systems. IRS will complete the BDNA deployment by October 2012. Once deployed, enterprise assets will be provisioned with BDNA credentials and BDNA will assist in building an accurate and complete hardware and software inventory for the Knowledge Incident/Problem Service Asset Management (KISAM) system. BDNA will provide data in accordance with National Institute of Standards and Technology (NIST) 800-40, section 2.2.1, that addresses information technology Inventory for network port, software configuration, and hardware configuration.

IMPLEMENTATION DATE: October 1, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should ensure that the IRS takes an enterprise-wide approach to buying tools to avoid redundancy and excessive cost, and develops an approach for using the data collected by its enterprise tools to support its patch management program, (including data collected by the BDNA and the DDMA).

CORRECTIVE ACTION #2: We agree with this recommendation. With respect to the first part of this recommendation relating to the enterprise-wide purchase of tools, the Enterprise Services function within our Information Technology (IT) organization ensures that products are selected based on enterprise solutions through the IT Configuration Control Board (IT CCB). Tools are, and shall continue to be, analyzed for redundant and duplicate features. Where possible, redundant tools shall be eliminated before new tools are approved for use. Where duplication or redundancy is required to provide either defense in depth or defense in breadth, this need shall be reflected in the usage guidance in the tools record within the Enterprise Standards Profile. The Change Request process, subservient to the IT CCB process, ensures that an engineering analysis of tools is conducted to avoid redundancy and excessive cost. This is a current and ongoing process. Therefore, we consider this part of the corrective action to be closed.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Attachment

Draft Audit Report –An Enterprise Approach Is Needed to Address the Security Risk of
Unprotected Patched Computers (Audit # 201220006 (e-trak # 2012-34847)

With respect to the second part of this recommendation relating to the development of an approach for using the data collected by enterprise tools to support patch management, the Enterprise Services, Cybersecurity, and Enterprise Operations functions within our IT organization will develop an approach to utilize the data from various sources to ensure that the patch management program is efficient and effective. This approach will include the collection of data, analysis of patching requirement and preparing an implementation plan. The proposed implementation date is provided below.

IMPLEMENTATION DATE: April 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Chief Technology Officer should update patch management policy to provide clear expectations for when patches must be installed based on criticality.

CORRECTIVE ACTION #3: We agree with this recommendation. The IRS will update the patch management policy in Internal Revenue Manual 10.8.50, providing clear standards for timeliness of patch installation based on criticality.

IMPLEMENTATION DATE: February 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Technology Officer should implement procedures to hold system owners accountable for patching computers within prescribed time periods.

CORRECTIVE ACTION #4: We agree with the spirit and intent of the recommendation. We believe that our existing procedures address this recommendation.



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Attachment

Draft Audit Report –An Enterprise Approach Is Needed to Address the Security Risk of Unprotected Patched Computers (Audit # 201220006 (e-trak # 2012-34847)

IMPLEMENTATION DATE: Not Applicable

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #5: The Chief Technology Officer should establish patch performance metrics in terms of setting compliance rate goals and measure them on a monthly basis.

CORRECTIVE ACTION #5: We agree with the spirit and intent of this recommendation. The IRS will update the patch performance metric policy in Internal Revenue Manual 10.8.50, providing clear standards for timeliness of patch installation based on a risk assessment of criticality. We will collect measurement performance metrics and establish a periodic monitoring process.

IMPLEMENTATION DATE: February 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #6: The Chief Technology Officer should implement enterprise-level responsibility to set and enforce IRS patch management policy to include deployment of enterprise patch management tools that automate patch installation and monitoring for like operating systems and software.

CORRECTIVE ACTION #6: We agree with this recommendation. The IRS will update the patch management policy in Internal Revenue Manual 10.8.50 to set patch management standards. The Cybersecurity function within our IT organization will have responsibility for ensuring enterprise-wide compliance with patch management policies. Cybersecurity will partner with other functions in our IT organization as well as with other IRS business and operating divisions to accomplish this corrective action.

IMPLEMENTATION DATE: April 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity



*An Enterprise Approach Is Needed to Address
the Security Risk of Unpatched Computers*

Attachment

Draft Audit Report –An Enterprise Approach Is Needed to Address the Security Risk of
Unprotected Patched Computers (Audit # 201220006 (e-trak # 2012-34847)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #7: The Chief Technology Officer should correct the issues with Altiris patch management tool reporting capabilities.

CORRECTIVE ACTION #7: We agree with this recommendation. Currently the reporting module of our enterprise Patching Solution (Altiris) does not support the consolidation of information across our patching nodes. To address this recommendation, we will engage the Altiris vendor to develop an enterprise-level reporting capability. In the interim, we have taken steps to extract the data from multiple nodes and collect it in a repository to facilitate the presentation of an enterprise view.

IMPLEMENTATION DATE: September 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #8: The Chief Technology Officer should complete implementation of controls to ensure that unsupported operating systems are not putting the IRS at risk.

CORRECTIVE ACTION #8: We agree with this recommendation. The Enterprise Services function within our IT organization will ensure that only supported operating systems are in use at the IRS through the use and monitoring of the Universal Configuration Management Database (UCMDB). Unsupported operating systems will be identified, the owners will be notified, and corrective actions taken to remove or replace the systems in order to prevent and reduce risks to IRS networks.

The implementation due date is dependent on the successful deployment of UCMDB, with a target completion date of July 1, 2013.

IMPLEMENTATION DATE: July 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services