



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

**September 21, 2006**

**Reference Number: 2006-20-167**

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(b) = Law Enforcement Guideline(s)

7 = Predecisional Staff Recommendations or Suggestions to Agency Decision Makers

8 = Information Reflecting the Bureau's Decision-making Processes



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

September 21, 2006

**MEMORANDUM FOR** ACTING CHIEF INFORMATION OFFICER

**FROM:** *Michael R. Phillips*  
Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk (Audit # 200520035)

This report presents the results of our review to assess the effectiveness of the Internal Revenue Service's (IRS) practices for ensuring the identification and installation of security updates for computer systems and applications.

*Impact on the Taxpayer*

When vendors identify security flaws with their systems, they make security patches<sup>1</sup> available to be installed on their customers' computers. The IRS process for installing patches has not ensured all of its 100,000 computers have been adequately protected. As a result, sensitive taxpayer information is more susceptible to unauthorized disclosure to hackers and unethical employees and contractors, and computer systems are more vulnerable to disruptions of operations that could jeopardize and waste taxpayer dollars.

*Synopsis*

In May 2004, the IRS suffered one of its most significant computer security incidents when the Sasser Worm<sup>2</sup> propagated itself throughout the entire IRS computer network. The incident could have been avoided if an available security patch had been installed on infected systems.

---

<sup>1</sup> 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.

<sup>2</sup> The Sasser Worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computers. It also probed for other computers to infect. This Worm rendered computers inoperable.



## *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk*

Operational organizations within the IRS were notified numerous times by the Office of Mission Assurance and Security Services to install the patch from April 14, 2004, when the patch became available, through May 2, 2004, when the Worm first infected IRS systems. However, the patch was not applied to servers consistently and was not applied to any workstations. The Worm cost the IRS an estimated \$3.6 million in lost salaries and \$50.6 million in lost or delayed tax assessments and tax collections.<sup>3</sup>

From June 2001 through February 2006, we issued 11 reports containing patch management issues.<sup>4</sup> During our current and prior reviews, we found patch identification, testing, and monitoring efforts were generally adequate. The IRS has established a vulnerability and remediation group tasked with identifying software for improving the overall management of this process. Additionally, the IRS has implemented corrective actions related to patch management issues from our prior reports. Finally, during the aftermath of the Sasser Worm incident, the IRS conducted an internal review that identified breakdowns in procedures and recommended corrective actions to prevent such events from recurring.

***Despite recent improvements to patch management practices, the IRS continues to have unpatched computers throughout its infrastructure.***

Although the IRS has made commendable progress towards improving its patch management processes, controls over patch implementation continue to allow unpatched systems. For example:

- The IRS' own monitoring efforts determined several essential security patches were not installed on Windows-based workstations and servers. An IRS report dated November 22, 2005, showed 33 critical patches were missing from a significant number of workstations and servers.
- Our review of the IRS' Common Operating Environment<sup>5</sup> noted 28 percent of the Windows workstations reviewed were missing security patches.
- Our review of the Tivoli<sup>®</sup> Software Suite<sup>6</sup> noted security patches were successfully installed only 67 percent of the time on Windows-based computers.
- Nine other reviews noted patches were not installed to varying degrees on various computer systems.

<sup>3</sup> The \$50.6 million estimate was identified by the IRS in its post-Sasser Worm evaluation soon after the incident occurred. The IRS has since stated that tax assessments and tax collections would have been processed by the IRS in subsequent tax periods and, therefore, do not represent actual losses.

<sup>4</sup> See Appendix IV for a list of the audit reports included in this review.

<sup>5</sup> See Appendix IV, Report 1.

<sup>6</sup> See Appendix IV, Report 2. Tivoli<sup>®</sup> is a registered trademark owned by International Business Machines.



## *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk*

---

The patches were not always installed for two primary reasons: the automated approach used to install patches on Windows-based systems did not always have valid connections to the systems requiring patching, and 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.

As for its internal review of the Sasser Worm incident, the IRS either took no corrective actions or did not complete corrective actions for 3 of the 10 recommendations. While the IRS has formed a group to develop stronger patch management controls, the scope of the group's work is limited and not designed to address the causes mentioned above. As of September 2005, the group estimated full implementation of the controls within its scope may not occur for an additional 12 months to 18 months.

Ineffective IRS patch management practices continue to put the IRS network at risk. The IRS continues to be exposed to network intrusions that could result in enormous financial impact related to lost or delayed tax assessments and collections and nonfinancial impact related to lost productivity, similar to the effects that occurred when the Sasser Worm infiltrated the IRS.

### *Recommendation*

Because we have included recommendations related to patch management issues in our prior audit reports and the IRS is taking actions to address patch management, we made no additional recommendations in this report. We will continue to monitor the IRS' patch management strategy and report any actions taken to eliminate the risks or deficiencies identified in our future security-related reviews.

### *Response*

IRS management agreed with the facts in our report and noted they continue to take aggressive approaches towards improving the patch management process. The IRS has developed a self-install script (computer program) that identifies and installs patches on workstations and laptops. A nationwide roll out of this script is scheduled to be completed by February 2007. The IRS has also taken steps to improve the success rate of patch distributions to workstations. These steps include aggressive management of Tivoli<sup>®</sup> endpoints and considering an approach that would not allow workstations onto the network until missing patches are updated. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report finding. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.



---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

*Table of Contents*

**Background** .....Page 1

**Results of Review** .....Page 3

    Patch Installation Practices Continue to Result in Unpatched  
    Computer Systems .....Page 4

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 8

    Appendix II – Major Contributors to This Report .....Page 9

    Appendix III – Report Distribution List .....Page 10

    Appendix IV – Prior Treasury Inspector General for Tax Administration  
    Audit Reports With Security Patch Management Issues .....Page 11

    Appendix V – Management’s Response to the Draft Report .....Page 13



---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

*Abbreviations*

CIO	Chief Information Officer
COE	Common Operating Environment
CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service



---

## *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk*

---

### *Background*

A 2004 Computer Security Institute and Federal Bureau of Investigation survey<sup>1</sup> showed that 91 percent of the respondents believed their computer system intrusions could have been prevented if system administrators had implemented patches for countering known vulnerabilities. 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. While vendors try to address known security flaws immediately, a time gap occurs from when the problem becomes publicly known until the vendor prepares the update to correct the flaw and users install the update. This gap, which provides potential intruders an opportunity to take advantage of the known flaws and mount attacks on vulnerable computers and networks, is becoming increasingly shorter as technology increases and hackers get wiser.

***A patch is a fix of a design flaw in a computer program. When patches are not installed timely, hackers could exploit the unpatched weakness and assume control of a computer.***

For this reason, it is critical, particularly for high-risk security vulnerabilities, that organizations apply security patches as quickly as possible. The potential risk of an unpatched weakness varies, depending on the nature of the weakness. A hacker could exploit an unpatched weakness and take over control of a computer to access its contents (e.g., user accounts, password information), use the computer as a launching point to attack other computers, or simply damage the computer so no one else can use or access it.

The actual installation of a patch appears to be a simple task. However, two factors complicate and challenge this task. First, all computers to which the patch applies must be identified and patched. The larger the organization, the more computers are likely to exist and be affected by vulnerabilities. Second, there are thousands of vulnerabilities being identified each year. The CERT<sup>®</sup> Coordination Center<sup>2</sup> determined 5,990 security vulnerabilities were reported during 2005. Vulnerabilities are generally spread across different software products. The more types of software used within an organization, the more difficult the task of patching all affected software products becomes.

The Internal Revenue Service (IRS) is a large organization with almost 100,000 employees and is very reliant on automation and the use of computers to administer the nation's tax system. It

---

<sup>1</sup> The 2004 *Computer Crime and Security Survey* was conducted by the Computer Security Institute with participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The 2004 survey results were based on the responses of 494 computer security practitioners across the United States.

<sup>2</sup> The CERT<sup>®</sup> Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a Federally funded research and development center operated by the Carnegie Mellon University.



---

## *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk*

---

has over 100,000 computers containing various operating systems and applications. Consequently, the seemingly easy task of patching computers turns into a monumental effort.

Computer security patching can be segmented into four basic processes: identification, testing, distribution and installation, and monitoring and follow-up.

1. Patch identification involves actively monitoring vendor and other information sources for known vulnerabilities and their related patches.
2. Patch testing involves conducting tests on a patch to ensure there are no unintended consequences when the patch is installed on affected computers.
3. Patch distribution and installation involve ensuring patches get distributed to the appropriate functions and installed on all affected computers.
4. Patch monitoring and follow-up involve the active monitoring of systems, to identify any systems without required patches, and follow-up efforts to ensure patches ultimately get installed on these systems.

Various organizations within the IRS manage the patch process. The Computer Security Incident Response Center (CSIRC) within the Office of Mission Assurance and Security Services has primary responsibility for identifying and notifying the Chief Information Officer (CIO) and business unit organizations about the availability of patches. It also conducts patch monitoring and follow-up. Upon being notified of patches, system administrators from various functions under the CIO and business units conduct patch testing, installation, monitoring, and follow-up, depending on the type of computer and user. For example, the End User Equipment and Services organization under the CIO is responsible for end-user computers, so it is also responsible for testing, installing, and following up on patches for IRS employees' computers.

This review was performed in the office of the CIO at the IRS National Headquarters in Washington, D.C., and New Carrollton, Maryland, during the period November 2005 through April 2006. This review also relied on results presented in 11 of our security-related audit reports issued from June 2001 through February 2006.<sup>3</sup> The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

<sup>3</sup> See Appendix IV for a list of the audit reports included in this review.





---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

## *Results of Review*

In May 2004, the IRS suffered one of its most significant computer security incidents when the Sasser Worm<sup>4</sup> propagated itself throughout the entire IRS computer network. The incident could have been avoided if an available security patch had been installed on infected systems. Operational organizations within the IRS were notified numerous times to install the patch from April 14, 2004, when the patch became available, through May 2, 2004, when the Worm first infected IRS systems. However, the patch was not applied to servers consistently and was not applied to any workstations. The Worm cost the IRS an estimated \$3.6 million in lost salaries and \$50.6 million in lost or delayed tax assessments and tax collections.<sup>5</sup>

During our current and prior reviews, we found patch identification, testing, and monitoring efforts were generally adequate. For example:

- Patch identification processes were generally in place and operating effectively. The CSIRC was primarily responsible for monitoring the computer industry and maintaining contacts with major computer vendors to identify when vulnerabilities become known and for evaluating the criticality of available security patches for the entire IRS. The CSIRC then notified IRS functions of existing vulnerabilities and the related security patches. The criticality of vulnerabilities and patches was based on risk, with the highest risk vulnerabilities requiring patching within 72 hours from when they were identified by the IRS.
- Patch testing procedures had been established and were in place. Once the patches became available, the appropriate IRS functions would test the patches to ensure they did not detrimentally affect existing systems. After the patches passed testing, they were distributed for installation on appropriate systems.
- Patch monitoring efforts were identifying unpatched systems effectively. IRS functions monitored systems using various methods. Windows-based systems were perpetually scanned for missing patches. An internal computer program<sup>6</sup> was used for scanning non-Windows systems. The CSIRC also conducted periodic scanning for vulnerabilities.

---

<sup>4</sup> The Sasser Worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computers. It also probed for other computers to infect. This Worm rendered computers inoperable.

<sup>5</sup> The \$50.6 million estimate was identified by the IRS in its post-Sasser Worm evaluation soon after the incident occurred. The IRS has since stated that tax assessments and tax collections would have been processed by the IRS in subsequent tax periods and, therefore, do not represent actual losses.

<sup>6</sup> The Law Enforcement Manual Checker is an internally developed software suite designed to scan computer systems to ensure compliance with various computer security standards required by the IRS.



---

## *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk*

---

During Fiscal Year 2005, the IRS established a vulnerability and remediation group tasked with identifying software for improving the overall management of the patching process. This group includes managers and technicians from IRS computer security and operations functions. During the first phase of this project, the group identified whether any vendor software existed that could improve the IRS patch management process. The second phase of this project would involve implementing any software procured.

Additionally, the IRS has implemented corrective actions from our prior reports containing patch management issues. For example, the IRS established procedures for identifying, testing, and monitoring security patches. Finally, the IRS conducted an internal review during the aftermath of the Sasser Worm incident. This review identified breakdowns in procedures and recommended corrective actions to prevent such an occurrence from happening again. These issues included breakdowns in the communication and implementation processes that have since been addressed.

Although the IRS has made commendable progress towards improving its patch management processes, controls over patch installation continue to require attention.

### ***Patch Installation Practices Continue to Result in Unpatched Computer Systems***

The IRS installs patches on its computers either through automated processes or by having system administrators manually apply the patches to specific servers or workstations under their control. However, these processes did not always ensure required patches were installed on all computers. We identified the following problems with patch installation:

- The IRS' own monitoring efforts determined that several essential security patches were not installed on Windows-based workstations and servers. An IRS report dated November 22, 2005, presented the results of patch scanning conducted on 4,060 Windows servers and 95,034 Windows workstations; it showed that 33 critical patches were missing from both workstations and servers. Overall, the report showed there were 9,478 occurrences of 1 or more of these 33 patches missing from the 4,060 servers. The report also showed 227,976 occurrences of 1 or more of these 33 patches missing from the 95,034 workstations. The IRS requires that critical patches be distributed for installation on systems within 72 hours from when they are identified by the IRS. While some of these missing patches may have been superseded by subsequent patches, the overall results demonstrate that many systems continue to go unpatched.

***Despite recent improvements to patch management practices, the IRS continues to have unpatched computers throughout its infrastructure.***



## **Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk**

- In an effort to ensure consistency across the IRS network and to improve overall security of employee workstations, the IRS created the Common Operating Environment (COE), which is a standardized set of commercial-off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. As part of this effort, the IRS creates biannual COE updates, which contain the latest security patches for installation to employee workstations. Our review of the IRS' COE<sup>7</sup> noted 28 percent of the Windows workstations reviewed did not have the latest COE update installed. By not having the latest COE update, these workstations were missing 16 security patches, 6 of which were considered high risk by IRS standards.
- From an automated enterprise approach, the IRS uses the Tivoli<sup>®8</sup> applications, which provide it with the ability to systemically deliver the most current versions of software and updated security patches to employees' computers and to scan the network for maintaining accurate computer inventory records. Our review of the IRS' use of the Tivoli<sup>®</sup> Software Suite<sup>9</sup> noted security patches were successfully installed only 67 percent of the time on Windows-based computers. We found several security patch distributions with success rates below 50 percent, with some succeeding in as few as 18 percent of the instances.
- Nine other reviews conducted since 2001 noted patches had not been installed to varying degrees on various systems. For example:

➤ 7,8,2(b)

➤

Security patches were not always installed for two primary reasons:

- The automated approach used to install patches on Windows-based systems did not always have valid connections to the systems requiring patching.
- System administrators did not always install patches due to the effect they believed such patches would have on systems under their control or due to the labor-intensive process of manually installing patches on systems.

<sup>7</sup> See Appendix IV, Report 1.

<sup>8</sup> Tivoli<sup>®</sup> is a registered trademark owned by International Business Machines.

<sup>9</sup> See Appendix IV, Report 2.

7,8,2(b)



## ***Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk***

The IRS responded to the aftermath of the Sasser Worm incident with a review that presented 10 findings and recommended corrective actions.

While the IRS has formed the aforementioned vulnerability and remediation group to develop stronger patch management controls, the scope of the group's work is limited and not designed to address the causes previously discussed. As of September 2005, the group estimated full implementation of the controls within its scope may not occur for an additional 12 months to 18 months.

Ineffective IRS patch management practices continue to put the IRS network at risk. The IRS continues to be exposed to network intrusions that could result in enormous financial impact related to lost or delayed tax assessments and collections and nonfinancial impact related to lost productivity, similar to the effects that occurred when the Sasser Worm infiltrated the IRS.

### ***Recommendation***

Because we have included recommendations related to patch management issues in our prior audit reports and the IRS is taking actions to address patch management, we are making no additional recommendations at this time. We will continue to monitor the IRS' patch management strategy and will report any actions taken to eliminate the risks or deficiencies identified in our future security-related reviews.

***Management's Response:*** IRS management agreed with the facts in our report and noted they continue to take aggressive approaches towards improving the patch management process. The IRS has developed a self-install script (computer program) that identifies and installs patches on workstations and laptop computers. A nationwide



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

roll out of this script is scheduled to be completed by February 2007. The IRS has also taken steps to improve the success rate of patch distributions to workstations. These steps include aggressive management of Tivoli® endpoints and considering an approach that would not allow workstations onto the network until missing patches are updated.



---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to assess the effectiveness of the IRS' practices for ensuring the identification and installation of security updates for computer systems and applications. To accomplish our objective, we:

- I. Determined whether the IRS effectively distributed and installed patches by consulting with appropriate staff and reviewing documentation, including IRS scans of Windows-based servers and workstations.
- II. Determined whether the IRS effectively tested patches prior to installation to applicable computing devices by identifying and evaluating the testing process.
- III. Determined whether the IRS effectively followed up on patch installation and proactively identified unpatched computers by consulting with appropriate organizations and reviewing documentation.
- IV. Determined the status and progress of IRS actions to address issues related to the Sasser Worm<sup>1</sup> by consulting with appropriate offices and reviewing relevant documentation.
- V. Determined the status and progress of IRS actions to address recommendations from eight Treasury Inspector General for Tax Administration reports issued from Fiscal Years 2001 through 2004 that contained issues related to patch management.
- VI. Reviewed the results from three Treasury Inspector General for Tax Administration reports issued after Fiscal Year 2004 that contained issues related to patch management. We did not review IRS actions to address the recommendations contained in these three reports because corrective actions had not been completed at the time of our review.
- VII. Determined the status of the IRS vulnerability and remediation group for addressing security patch issues.

---

<sup>1</sup> The Sasser Worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computers. It also probed for other computers to infect. This Worm rendered computers inoperable.



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

**Appendix II**

*Major Contributors to This Report*

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)  
Kent Sagara, Acting Director  
Joseph Cooney, Acting Audit Manager  
Bret Hunter, Lead Auditor  
Jody Kitazono, Senior Auditor  
Larry Reimer, Senior Auditor



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Chief, Mission Assurance and Security Services OS:MA  
Deputy Chief Information Officer OS:CIO  
Associate Chief Information Officer, End User Equipment and Services OS:CIO:EU  
Associate Chief Information Officer, Enterprise Networks OS:CIO:EN  
Associate Chief Information Officer, Enterprise Operations OS:CIO:EO  
Director, Information Security OS:CIO:IS  
Director, Enterprise Systems Management OS:CIO:EU:ESM  
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, Program Oversight OS:CIO:SM:PO





---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

**Appendix IV**

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

The following Treasury Inspector General for Tax Administration audit reports contain patch management issues.

1. *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006).
2. *Progress Has Been Made on Using the Tivoli<sup>®</sup> Software Suite,<sup>1</sup> Though Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories* (Reference Number 2006-20-021, dated December 2005).
3. *The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made* (Reference Number 2005-20-143, dated September 2005).
4. *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2004-20-073, dated April 2004).
5. *Key Security Controls of the Criminal Investigation Management Information System Have Not Been Implemented* (Reference Number 2004-20-081, dated March 2004).
6. *Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses* (Reference Number 2004-20-027, dated January 2004).
7. *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (Reference Number 2003-20-118, dated July 2003).
8. *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003).

---

<sup>1</sup> Tivoli<sup>®</sup> is a registered trademark owned by International Business Machines.



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

9. *Controls Over the Excise Files Information Retrieval System Website Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2002-20-064, dated April 2002).
10. *Controls Over the Procurement Website Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2002-20-045, dated January 2002).
11. *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001).



*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

**Appendix V**

*Management's Response to the Draft Report*




CHIEF INFORMATION OFFICER

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

RECEIVED  
SEP 14 2006

SEP 14 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez  
Acting Chief Information Officer 

SUBJECT: Management Response to Draft Audit Report – Uninstalled  
Computer Security Patches Continue to Put Computer Systems  
at Risk (Audit #200520035) (i-trak #2006-15494)

Thank you for the opportunity to review and comment on your draft report. The report acknowledges that the IRS has made commendable efforts towards improving our patch management process, and that during this and prior reviews, our patch identification, testing, and monitoring efforts were generally adequate. We appreciate that feedback. The report also states that the Sasser Worm cost the IRS an estimated \$50.6 million in lost or delayed tax assessments and tax collections. As noted, this figure does not represent actual losses, but rather delayed receipts due to tax assessment and collections being processed in subsequent tax periods.

Patching over 100,000 computers with various operating systems and applications is a monumental effort. While we have made great strides in improving the patch management process, we continue to explore more aggressive means. For example, the IRS created a patch management self-install script, UpdateIT, which identifies and installs missing patches on workstations and laptops. We piloted UpdateIT across two territories and at the Maryland Technology Center and achieved an 80% reduction in missing patches. The remaining 20% were primarily non-Microsoft patches labeled "non-critical" according to the Computer Security Incident Response Center (CSIRC). Due to the pilot's success, a nationwide rollout of UpdateIT is currently underway and will be completed by February 1, 2007.

The IRS has also developed a standardized workstation patch distribution process that has increased successful patch deployment from an average of 85% in Fiscal Year (FY) 2005 to 90% in FY 2006. Since 93-94% is regarded as maximum penetration via the Tivoli tool in our current environment, we are taking a two-pronged approach regarding failed patches:



---

*Uninstalled Computer Security Patches  
Continue to Put Computer Systems at Risk*

---

2

1. We are aggressively managing Tivoli® endpoints to reduce the number of unreachable targets by ensuring inactive workstations are not included on the target list, and that active workstations have healthy endpoints.
2. We are exploring a variation of UpdateIT as part of the logon script. This would prevent any workstation from accessing the network until missing patches are updated.

In response to the Sasser Worm incident, we established an Emergency First Response Team (EFRT) to mobilize quickly in the event of future data security incidents. During November/December 2005, the EFRT responded successfully to two separate incidents and contained the number of infected workstations to 40-50. These workstations were rectified within a matter of hours with no significant interruption to operations.

We appreciate the valuable assistance and guidance that your team provides. We continue to be fully committed to securing our computer environment by evaluating current processes, promoting user awareness, educating our desktop support personnel, and applying innovative ideas to increase our compliance.

If you have any questions, please contact me at (202) 622-6800 or members of your staff may contact Judith Mills, Director of Program Oversight, at (202) 283-4915.