TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat

March 10, 2009

Reference Number: 2009-20-045

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

March 10, 2009

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat (Audit # 200820014)

This report presents the results of our review of malware prevention and response controls. The overall objective of this review was to determine whether adequate security controls are present to prevent and respond to malware attacks. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of our statutory requirements to annually review the adequacy and security of Internal Revenue Service (IRS) information technology.

Impact on the Taxpayer

Malware, also known as malicious code or malicious software, refers to a computer program that is inserted into a computer system with the intent of compromising the confidentiality, integrity, or availability of an organization's data, applications, or operating systems. The IRS' preventive and response controls to address malware are generally effective, but continued attention should be given to 1) limiting some practices that increase the risk of a malware incident[1] and 2) increasing employees' awareness of their responsibilities for preventing a malware incident. Without ongoing attention in these areas, IRS computers and the sensitive taxpayer data stored on them are at risk of compromise that could ultimately result in theft of taxpayer identities and fraud.

[1] A successful malware incident is one in which the code successfully installs itself on the target computer and can begin executing to accomplish its intended objective.

Synopsis

Malware is a threat that affects all computer system users and is an evolving challenge that is difficult to combat because new malware is written faster than ever before. Malware can be written to disrupt computer system operations, commit identity theft and credit card fraud, and monitor user activity. During Calendar Year 2008, the IRS responded to 961 malware incidents, an increase of 45 percent over the prior year.

The Computer Security Incident Response Center (CSIRC) is responsible for providing the IRS with a team of capable "first responders" organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computing assets. We determined that the CSIRC's responses to malware incidents were timely and thorough.

To prevent the introduction of malware, the IRS must provide current antivirus software for all workstations and servers, take actions to limit risky practices, and provide regular employee awareness training. Workstations are automatically scanned weekly. However, only 89 percent of IRS servers were scanned weekly. The remaining servers were scanned less frequently or not at all. The introduction of malware on servers is particularly risky because many users access them, making the spread of the malware to other computer systems more likely.

The IRS had adequately implemented many of the enhanced controls outlined in a December 2007 Department of the Treasury memorandum[2] to block known malicious sites and prohibit administrator accounts from receiving email from accounts outside of the Department. The IRS is also adequately preventing access to online email accounts outside of the Department for all user accounts, in compliance with its own policy.

The Department of the Treasury memorandum also prohibits administrators from using their administrator accounts to access the Internet unless authorized in writing by the Bureau Chief Information Officer or his or her designee. The Internet is a primary source for malware infections, and administrator accounts are particularly attractive to persons wanting to cause harm to the IRS because the accounts have powerful privileges such as adding users and modifying configurations. If these accounts were infected with malware, unauthorized persons could obtain the same privileges and do malicious damage to the IRS computer network. We identified 63 administrator accounts that had successfully accessed Internet web sites a total of 820 times in a 1-week period. None of these accounts were authorized to access the Internet by the IRS Chief Information Officer. Non-administrator accounts could have been used to accomplish the same purposes without increasing the risk of a malware infection.

Our review of malware incidents reported in Calendar Year 2007 showed that the incidents were caused by IRS employees engaging in activities that increase the risk of malware infection, such

[2] Department of the Treasury memorandum "Enhanced Cyber Security Controls," dated December 20, 2007.

as using removable storage devices, downloading software, and opening attachments or links in email. The CSIRC does not routinely contact users when their authorized system activity results in a successful malware incident or when the incident is caused by a violation of IRS policy. We believe that informing users of their specific activities that resulted in malware infections would serve to supplement and personalize the mandatory annual security training provided to employees and better educate users about the malware threat. In addition, while the mandatory annual security training for IRS employees and contractors includes common ways in which users can infect systems with malware, it does not include a thorough list of the actions that have led to malware infections on IRS systems.

Recommendations

We recommended that the Chief Information Officer 1) schedule automatic scans of antivirus software on servers, 2) regularly remind administrators not to use their administrator accounts to access the Internet and monitor Internet activity to determine whether administrators are complying with this control, 3) notify employees and their managers when their activity results in a successful malicious code incident, particularly when the activity is a violation of IRS policy, and 4) update the IRS security awareness training to include the use of portable and removable media among the common ways in which users can introduce malicious code to the network and the potential effects.

Response

IRS management agreed with our recommendations and will schedule automated antivirus scans on servers, use the Symantec™ Antivirus console to regularly monitor servers to ensure that antivirus scans are executed weekly, and ensure that administrators are regularly reminded of Internet access restrictions. The CSIRC will continually monitor the enterprise content filtering solution for Internet access by administrator accounts, regularly report violations of Internet access by administrators to the Cybersecurity Operations organization and IRS Security Offices for followup actions, and ensure that employees and their managers are notified regarding applicable incidents. Finally, the IRS will use the security awareness training course mandated by the Department of the Treasury that addresses the proper use of portable and removable media. Management's complete response to the draft report is included as Appendix IV.

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

Table of Contents

Appendices

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
US-CERT	United States Computer Emergency Readiness Team

Background

Malware, also known as malicious code or malicious software, refers to a computer program that is inserted into a computer system with the intent of compromising the confidentiality, integrity, or availability of an organization's data, applications, or operating systems. Malware can infect computers in a variety of ways. For example, viruses are self-replicating programs that are often inserted into computer software or data files through user interaction, such as opening a file or running a program. In contrast, trojan horses are self-contained, non-replicating programs that appear to be legitimate programs but that have been replaced or inserted with hidden malicious code. Malware is delivered through commonly used applications and devices, such as email, the Internet, and portable media devices.

Malware is a threat that affects all computer system users and is an evolving challenge that is difficult to combat because new malware is written faster than ever before. A recent report by F-Secure® notes that as much malware was produced in 2007 as was produced in the previous 20 years combined, based on its detections.[1] Similarly, Symantec™ reports that, based on its research, there are indications that the rate of malware creation might be exceeding that of legitimate software applications.[2] Malware is also difficult to combat because it is delivered through basic, mission-critical applications such as web browsers and email. For example, in August 2008, emails claiming to be CNN or MSNBC news alerts were sent to millions of email accounts in an attempt to lure victims into downloading malware from compromised web sites.

Malware can be written to disrupt computer system operations, commit identity theft and credit card fraud, and monitor user activity. However, not all malware is driven by financial motives. In 2006, hackers stole data from the United States Department of State computer network after a Department of State employee in Asia opened an email that allowed the hackers to break into the Federal Government's computer system. The incident caused all of the Department of State's Internet connections throughout eastern Asia to be severed.

Within the Internal Revenue Service (IRS), the Computer Security Incident Response Center (CSIRC) responds to malicious code incidents. The CSIRC is responsible for providing the IRS with a team of capable "first responders" organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computing assets.

The IRS CSIRC also shares information regarding malicious web sites it identifies with other Federal Government entities via the Government Forum of Incident Response and Security Teams to enable them to proactively restrict access before they are victimized. From April 1 to

[1] F-Secure® Data Security Wrap-Up 2007.
[2] Symantec™ Internet Security Threat Report, Trends for July–December 2007, Volume XII, published April 2008.

June 30, 2008, the Federal Government entities comprising the Government Forum of Incident Response and Security Teams blocked 1,228 malicious web sites. The CSIRC provided the initial intelligence on 461 (38 percent) of these web sites.

Based on incident data obtained from the CSIRC, the number of malware incidents within the IRS continues to rise each year, as does the IRS' success in preventing malware infection. During Calendar Year 2008, the IRS responded to 961 malware incidents, an increase of 45 percent over the prior year.

To address the malware threat, organizations must implement controls to prevent, detect, and respond to malware. This review focused on the IRS' efforts in preventing and responding to malware. An evaluation of IRS malware detection controls could be included in a subsequent audit.

This review was performed at the IRS National Headquarters in Washington, D.C., in the Office of Cybersecurity during the period October 2007 through September 2008. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Internal Revenue Service Responded Appropriately When Malware Was Detected

Responding to security incidents is one of the CSIRC's primary responsibilities. CSIRC analysts actively monitor a wide variety of sources such as intrusion detection systems, firewalls, and audit logs to identify potential malicious code incidents. During Calendar Year 2007, the CSIRC identified and responded to 661 malicious code incidents. Once an incident was identified, CSIRC analysts conducted a thorough analysis to determine the source, nature, and purpose of the malicious code. The analysts expeditiously coordinated with the Modernization and Information Technology Services organization and provided instructions for containing and eradicating the malware to protect IRS systems and data from further infection. When possible, the analysts also took appropriate steps to prevent future infections by blocking malware-infected Internet sites. The CSIRC's responses to the incidents we reviewed were timely and thorough.

Controls to Prevent the Introduction of Malware Can Be Improved

Without sufficient controls to prevent the introduction of malware, IRS computers and the sensitive taxpayer data stored on them are at risk of compromise that could ultimately result in theft of taxpayer identities and fraud. To prevent the introduction of malware, large organizations like the IRS must provide current antivirus software for all workstations and servers, take actions to limit risky practices, and provide regular employee awareness training.

Although the IRS effectively implemented antivirus controls for workstations, controls for servers can be improved

While there are numerous ways to help prevent malware from infecting computers, often the last line of defense is antivirus software, which the IRS requires to be installed on all of its computers running the Windows operating system. The IRS also requires antivirus scans to be performed at least weekly.

The IRS' antivirus implementation was generally adequate. The IRS has an adequate process in place to ensure that antivirus software is installed on its workstations and servers. For workstations, which include desktop and laptop computers, virus scans are scheduled to run weekly. If a computer is not on the network when the scan is conducted, the scan begins once the computer logs on to the network. The IRS is updating its computers with new virus signatures[3] in a timely manner, with 96 percent of IRS workstations updated within 2 business days and almost 100 percent updated within 1 week of a new signature being identified.

For servers, virus scans are not automated and must be manually initiated by the system administrators. Our analysis of antivirus scans conducted over an 8-week period from May 1 to June 30, 2008, determined that 89 percent of the servers were usually scanned weekly. The remaining servers were scanned less frequently or not at all because the system administrators did not always carry out this responsibility. The introduction of malware on servers is particularly risky because many users access them, making the spread of the malware to other computer systems more likely.

Attention is needed to ensure that administrator account access to the Internet is eliminated

Antivirus software alone is not sufficient to combat the evolving malware threat. In December 2007, the Department of the Treasury issued a memorandum[4] requiring enhanced security controls aimed at preventing practices that increase the risk of introducing malware. These enhanced controls include restrictions on use of administrator accounts[5] and blocking known malicious web sites.

The IRS has implemented many of the enhanced controls required by the Department of the Treasury. It has adequately implemented controls to block known malicious sites following United States Computer Emergency Readiness Team (US-CERT)[6] or Departmental notification of such sites. It is also adequately preventing access to online email accounts outside of the Department of the Treasury for all user accounts, in compliance with its own policy.

The Department of the Treasury memorandum also prohibits administrators from using their administrator accounts to receive email from accounts outside of the Department and from accessing the Internet unless authorized in writing by the Bureau Chief Information Officer or his or her designee. The Internet is a primary source for malware infections. To limit the risk of malware infection, system administrators should be assigned two types of accounts. One account should have the same privileges as those on the accounts for most other employees. The

[3] A virus signature is the binary pattern of the machine code of a particular virus. Antivirus programs compare their databases of virus signatures with the files on the hard disk and removable media to identify a virus. The antivirus vendor updates the signatures frequently and makes them available to customers via the Internet.

[4] Department of the Treasury memorandum "Enhanced Cyber Security Controls," dated December 20, 2007.

[5] An administrator account is a user account present on several popular network operating systems that has the highest level of control over a system and/or network. This account might have the ability to install hardware and software on the system; add, modify, or delete user accounts; and modify a system's security features.

[6] The US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, the US-CERT coordinates defense against and responses to cyber attacks across the nation.

other account should be used to carry out administrator responsibilities and should not be used for email or Internet access.

Administrator accounts are particularly attractive to persons wanting to cause harm to the IRS because the accounts have powerful privileges such as adding users and modifying configurations. If these accounts were infected with malware, unauthorized persons could obtain the same privileges and do significant damage to the IRS computer network. For IRS systems, malware can be used to steal taxpayer data, spy on IRS employee activities to gain access to IRS applications, and disrupt IRS computer operations.

The IRS is adequately preventing administrator accounts from receiving email from outside of the Department of the Treasury and has established procedures for assigning two accounts to administrators. However, in a 1-week period in February 2008, we identified 63 administrator accounts that successfully accessed Internet web sites a total of 820 times. These accesses appeared to be appropriate, with most accesses made to work-related sites. However, the administrator accounts were not authorized to access the Internet by the IRS Chief Information Officer. Non-administrator accounts could have been used to accomplish the same purposes without increasing the risk of a malware infection.

Although we found relatively few accesses by administrators, the scope of our review was limited to only a 1-week period. The IRS did not conduct sufficient monitoring to identify administrator accounts being used to access the Internet. As a result, we do not have assurance that accesses by administrator accounts are sufficiently controlled to prevent compromise by malware-infected sites.

Increased employee awareness of common causes of malware infections is needed

Because security products alone cannot protect systems from the threat of malware, employee awareness training is critical. If users are not sufficiently informed of the threats associated with their activities, they will likely continue to introduce malicious code into the IRS network.

Our review showed that the malware incidents reported in Calendar Year 2007 were caused by activities that increase the risk of malware infection, such as using removable storage devices, downloading software, and opening attachments or links in email. Of the 661 incidents reported in Calendar Year 2007, 311 were successful.[7] Of these, 216 (69 percent) were caused by accesses to the Internet. Most of the accesses were to authorized Internet sites. However, users were inadvertently redirected to malicious web sites.

[7] A successful malware incident is one in which the code successfully installs itself on the target computer and can begin executing to accomplish its intended objective.

As a result of these actions, the CSIRC found systems infected with malware in the form of viruses, worms, trojans, and spyware.[8] CSIRC analysts noted in their reviews of malware incidents that these types of malware have the potential to corrupt the integrity of the data, affect the availability of resources, disclose sensitive data, or further propagate throughout the enterprise.

The CSIRC does not routinely contact users when their authorized system activity results in a successful malware incident. Users are contacted when their use of removable media results in a malicious code infection, but they are not contacted for other common causes of malware. We believe that notifying users and informing them of their specific activities that resulted in malware infections would serve to supplement and personalize the mandatory annual security training and better educate users about the malware threat. Notification would make users more aware of the risks of Internet use and raise awareness that their Internet use can affect the performance of their responsibilities by disabling their computer system and possibly other systems on the IRS network.

The CSIRC does not have standard operating procedures to address malware incidents when they are caused by user policy violations. The CSIRC responses address the malicious code but do not always address the policy violation that caused the malicious code. As a result, policy violations that can lead to malware infections are inconsistently handled. The policy violations we identified included using personal portable hard drives, downloading unauthorized software, and accessing unauthorized Internet sites. For some incidents caused by using personal portable hard drives, the CSIRC ensured that the user was contacted and counseled about IRS policy. However, we identified 23 successful and unsuccessful malicious code incidents caused by users violating IRS information technology resources and security policies that were closed without the users being contacted or counseled about their actions. We believe that the CSIRC has a responsibility to notify employees and their managers when their actions violate IRS policies.

IRS employees and contractors are required to annually certify that they have completed the IRS Information Protection Mandatory Briefing, which includes security awareness refresher training. The mandatory annual security training for IRS employees and contractors covers common ways in which users can infect systems with malware. The IRS security awareness training should be updated to include a more thorough list of the actions that have led to malware infections on IRS systems. The training presentation lists the opening of virus-infected email attachments, installing software downloaded from the network, and linking to web sites

[8] A virus is a self-replicating program that is inserted into computer software or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. A worm is usually a small, self-contained and self-replicating computer program that invades computers on a network and usually performs a destructive action. A trojan is a self-contained, non-replicating program that, while appearing to be benign, actually has hidden malicious code. Trojan horses either replace existing files with malicious versions or add new malicious files. Spyware is software that collects information from computers and transmits it to third parties without the knowledge or informed consent of computer users.

containing malware as common ways in which users can infect systems with malware. However, the training does not include the use of personal portable devices and removable media as common ways in which users can infect systems with malicious code. Of the 661 malware incidents reported in 2007, 69 (10 percent) were caused by users inserting removable media such as compact discs or connecting external or portable hard drives to their systems.

Recommendations

The Chief Information Officer should:

Recommendation 1: Schedule automatic scans of antivirus software on servers.

> **Management's Response:** IRS management agreed with this recommendation. They will schedule automated antivirus scans on servers and will use the Symantec™ Antivirus console to regularly monitor servers to ensure that antivirus scans are executed weekly as required by the Internal Revenue Manual.

Recommendation 2: Regularly remind administrators not to use their administrator accounts to access the Internet and monitor Internet activity to determine whether administrators are complying with this control.

> **Management's Response:** IRS management agreed with this recommendation. They will issue regular reminders on Internet access restrictions for administrators by including information in mandatory annual security awareness training and by periodically publishing information in existing communication channels such as organizational webpages and newsletters. Management will also continually monitor the enterprise content filtering solution for Internet access by administrator accounts, regularly report violations to the Cybersecurity Operations organization and IRS Security Offices, conduct followup actions to validate the need for access, and remind administrators that such activity violates IRS policy.

Recommendation 3: Notify employees and their managers when their activity results in a successful malicious code incident, particularly when the activity is a violation of IRS policy.

> **Management's Response:** IRS management agreed with this recommendation. The Cybersecurity Operations organization will implement revised processes to facilitate the continued prevention, detection, and response to cyber incidents, while ensuring that employees and their managers are notified regarding applicable cyber incidents.

Recommendation 4: Update the IRS security awareness training to include the use of portable and removable media among the common ways in which users can introduce malicious code to the network and the potential effects.

> **Management's Response:** IRS management agreed with this recommendation. The IRS will convert to the Information Systems Security Line of Business awareness training

course (as mandated by the Department of the Treasury) that addresses the use of portable and removable media being among the common ways in which users can introduce malicious code to the network and the potential effects. Management will continue to review updates to the training course content to ensure that this topic is included in the final version.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether adequate security controls are present to prevent and respond to malware[1] attacks. We specifically reviewed the IRS' responses to incidents identified by the CSIRC for Calendar Year 2007.

The electronic data used in this review, with the exception of the CSIRC incident log, were source data extracted directly from IRS systems. The Government Accountability Office document *Assessing the Reliability of Computer-Processed Data* (GAO-03-273G, dated October 2002) provides that information system reviews are an exception that does not require data validation because the information system controls are tested as part of the review.

To accomplish our objective, we:

I. Determined whether the IRS had adequate procedures in place to respond to and eradicate malware identified on IRS computer systems.

   A. Identified the requirements for responding to and eradicating malware identified on IRS computer systems from sources such as the Internal Revenue Manual, National Institute of Standards and Technology[2] guidance, and the Department of the Treasury recommended Enhanced Cyber Security Controls.

   B. Assessed the adequacy of controls over malware incident response.

      1. Obtained a list of all malware incidents identified by the CSIRC for Calendar Year 2007.

      2. Determined whether the incident report was valid and complete.

      3. Determined whether IRS responses to incidents identified by the CSIRC followed IRS, Department of the Treasury, and other Federal Government requirements.

   C. Identified the reasons for inadequacy of responses to malware incidents.

   D. Assessed the effect of inadequate control weaknesses on responding to malware incidents.

[1] Malware, also known as malicious code or malicious software, refers to a computer program that is inserted into a computer system with the intent of compromising the confidentiality, integrity, or availability of an organization's data, applications, or operating systems.

[2] The National Institute of Standards and Technology, a Federal Government agency within the Department of Commerce, develops and issues standards, guidelines, and other publications to assist Federal Government agencies in protecting their information and information systems.

II. Determined whether the IRS had adequate controls in place to prevent malware from affecting IRS computers.

A. Identified the requirements for preventing malware from being introduced into the network from sources such as the Internal Revenue Manual, National Institute of Standards and Technology guidance, and the Department of the Treasury recommended Enhanced Cyber Security Controls.

B. Determined whether required controls to prevent malware had been implemented and were working properly.

1. Determined whether administrator accounts[3] are prohibited from web browsing and accessing other Internet connections outside of the IRS and the Department of the Treasury protected boundary, unless authorized in writing by the Chief Information Officer or his or her designee.
2. Determined whether administrator accounts are prohibited from receiving email from accounts outside of the Department of the Treasury, unless authorized in writing by the Chief Information Officer or his or her designee.
3. Determined whether known malicious sites, as identified to the Department of the Treasury from the US-CERT[4] or other sources, are blocked (inbound and outbound) at each Internet Access Point (unless explicit instructions are provided to Bureaus not to block specific sites). Blocking is to be accomplished within 2 business days following US-CERT or Departmental release of such sites.
4. Determined whether the IRS blocked access to online email sites.
5. Determined whether intrusion detection systems (or other functionally equivalent technology) are updated with new indicators/signatures[5] as they are made available by the US-CERT or the Department of the Treasury.

[3] An administrator account is a user account present on several popular network operating systems that has the highest level of control over a system and/or network. This account might have the ability to install hardware and software on the system; add, modify, or delete user accounts; and modify a system’s security features.
[4] The US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation’s Internet infrastructure, the US-CERT coordinates defense against and responses to cyber attacks across the nation.
[5] A virus signature is the binary pattern of the machine code of a particular virus. Antivirus programs compare their databases of virus signatures with the files on the hard disk and removable media to identify a virus. The antivirus vendor updates the signatures frequently and makes them available to customers via the Internet.

6. Determined whether antivirus software:

    a) Is installed on all IRS workstations and servers.

    b) Is updated with new virus signatures in a timely manner.

    c) Includes spyware[6] checking.

    d) Is periodically run on all IRS computers.

    e) Is updated and run each time an IRS computer connects to the IRS network.

    f) Scans all portable media connected to an IRS computer.

    g) Scans all incoming email.

C. Identified the reasons for inadequate malware prevention controls.

D. Assessed the effect of inadequate malware prevention controls.

[6] Spyware is software that collects information from computers and transmits it to third parties without the knowledge or informed consent of computer users.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Stephen Mullins, Director
Kent Sagara, Acting Director
Michael Howard, Audit Manager
Carol Taylor, Audit Manager
Alan Beber, Senior Auditor
Charles Ekunwe, Senior Auditor
Myron Gulley, Senior Auditor
Joan Raniolo, Senior Auditor

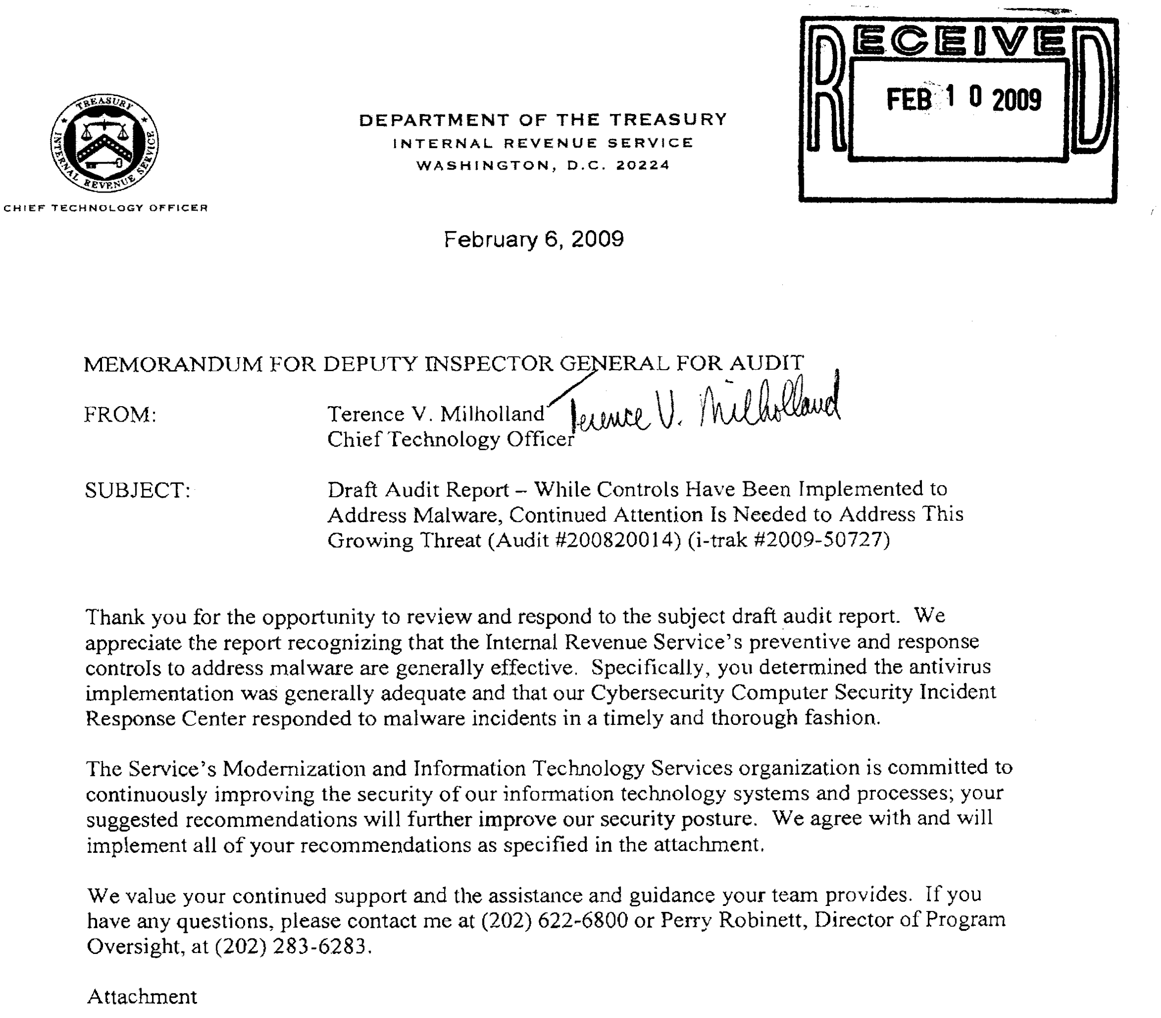
Appendix III

Report Distribution List

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

Appendix IV

Management's Response to the Draft Report



RECEIVED
FEB 10 2009

CHIEF TECHNOLOGY OFFICER

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

February 6, 2009

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

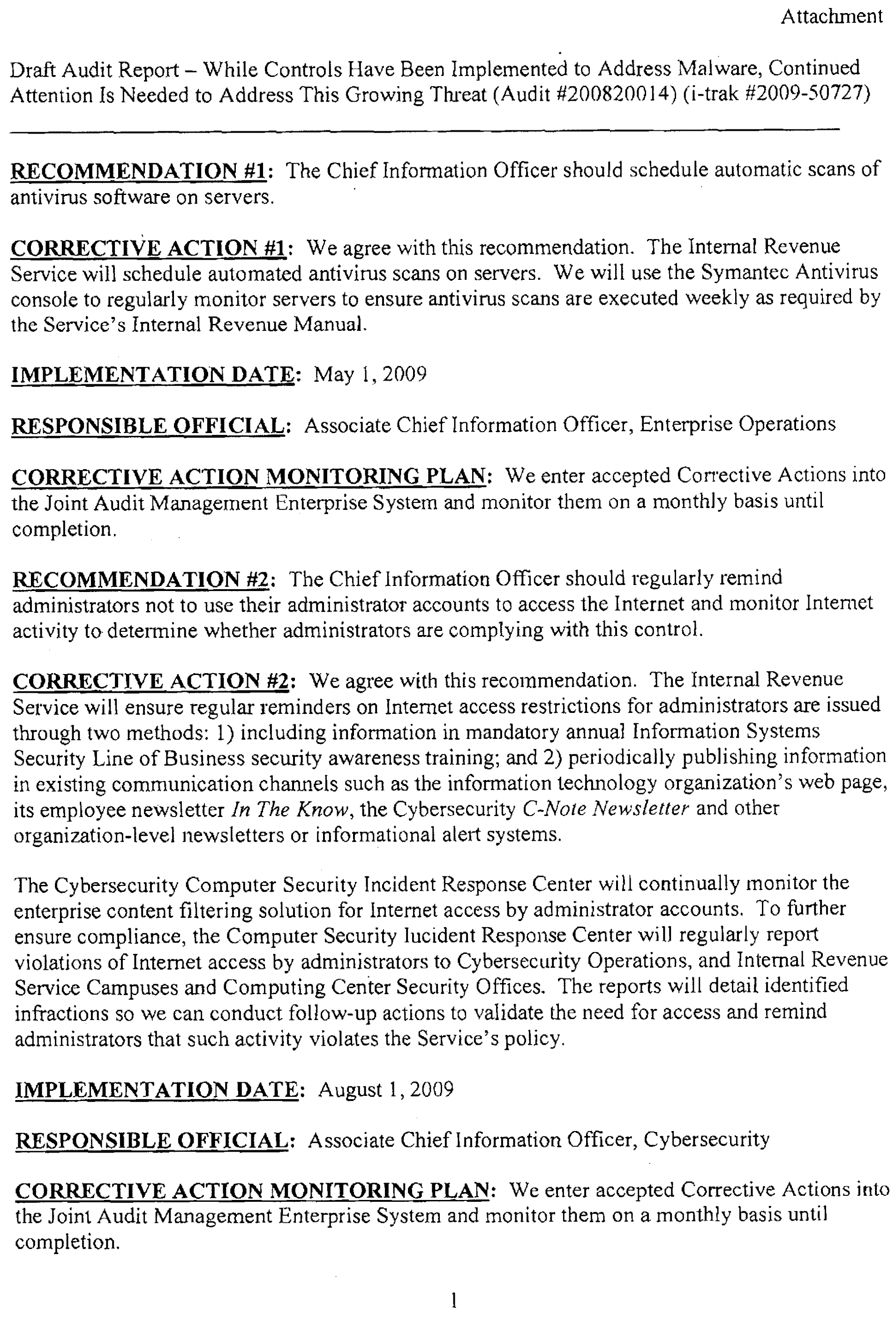
SUBJECT: Draft Audit Report – While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat (Audit #200820014) (i-trak #2009-50727)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate the report recognizing that the Internal Revenue Service's preventive and response controls to address malware are generally effective. Specifically, you determined the antivirus implementation was generally adequate and that our Cybersecurity Computer Security Incident Response Center responded to malware incidents in a timely and thorough fashion.

The Service's Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes; your suggested recommendations will further improve our security posture. We agree with and will implement all of your recommendations as specified in the attachment.

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

Attachment



Attachment

Draft Audit Report – While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat (Audit #200820014) (i-trak #2009-50727)

RECOMMENDATION #1: The Chief Information Officer should schedule automatic scans of antivirus software on servers.

CORRECTIVE ACTION #1: We agree with this recommendation. The Internal Revenue Service will schedule automated antivirus scans on servers. We will use the Symantec Antivirus console to regularly monitor servers to ensure antivirus scans are executed weekly as required by the Service's Internal Revenue Manual.

IMPLEMENTATION DATE: May 1, 2009

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 #2: The Chief Information Officer should regularly remind administrators not to use their administrator accounts to access the Internet and monitor Internet activity to determine whether administrators are complying with this control.

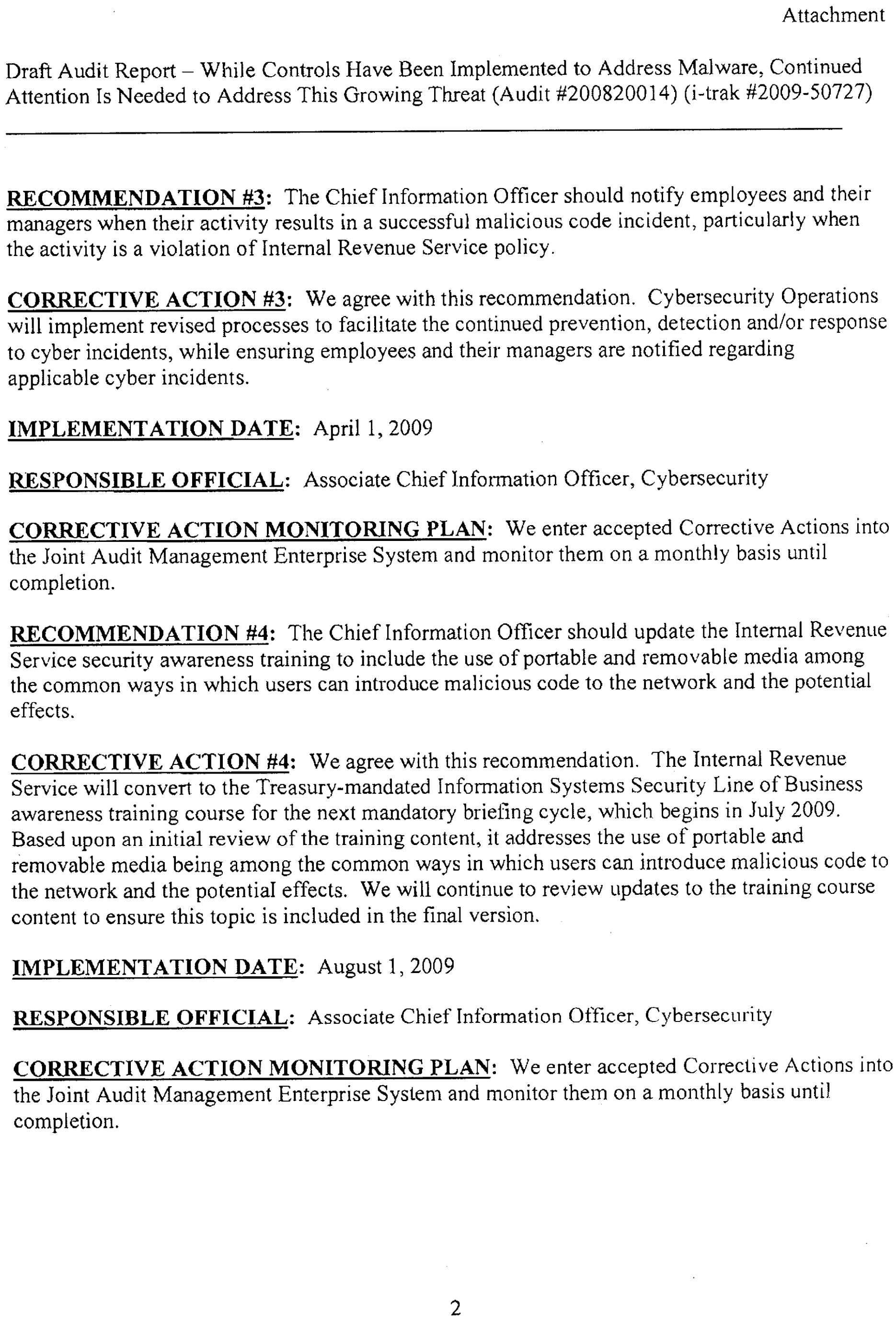
CORRECTIVE ACTION #2: We agree with this recommendation. The Internal Revenue Service will ensure regular reminders on Internet access restrictions for administrators are issued through two methods: 1) including information in mandatory annual Information Systems Security Line of Business security awareness training; and 2) periodically publishing information in existing communication channels such as the information technology organization's web page, its employee newsletter *In The Know*, the Cybersecurity *C-Note Newsletter* and other organization-level newsletters or informational alert systems.

The Cybersecurity Computer Security Incident Response Center will continually monitor the enterprise content filtering solution for Internet access by administrator accounts. To further ensure compliance, the Computer Security Incident Response Center will regularly report violations of Internet access by administrators to Cybersecurity Operations, and Internal Revenue Service Campuses and Computing Center Security Offices. The reports will detail identified infractions so we can conduct follow-up actions to validate the need for access and remind administrators that such activity violates the Service's policy.

IMPLEMENTATION DATE: August 1, 2009

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.



Attachment

Draft Audit Report – While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat (Audit #200820014) (i-trak #2009-50727)

RECOMMENDATION #3: The Chief Information Officer should notify employees and their managers when their activity results in a successful malicious code incident, particularly when the activity is a violation of Internal Revenue Service policy.

CORRECTIVE ACTION #3: We agree with this recommendation. Cybersecurity Operations will implement revised processes to facilitate the continued prevention, detection and/or response to cyber incidents, while ensuring employees and their managers are notified regarding applicable cyber incidents.

IMPLEMENTATION DATE: April 1, 2009

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 Information Officer should update the Internal Revenue Service security awareness training to include the use of portable and removable media among the common ways in which users can introduce malicious code to the network and the potential effects.

CORRECTIVE ACTION #4: We agree with this recommendation. The Internal Revenue Service will convert to the Treasury-mandated Information Systems Security Line of Business awareness training course for the next mandatory briefing cycle, which begins in July 2009. Based upon an initial review of the training content, it addresses the use of portable and removable media being among the common ways in which users can introduce malicious code to the network and the potential effects. We will continue to review updates to the training course content to ensure this topic is included in the final version.

IMPLEMENTATION DATE: August 1, 2009

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.