TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks

July 31, 2006

Reference Number: 2006-20-110

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 | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 31, 2006

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks (Audit # 200520032)

This report presents the results of our review to determine whether the Internal Revenue Service's (IRS) electronic mail (email) system was being used properly by employees and was secured by system administrators.

Synopsis

Email allows an organization and its employees to better communicate with each other, customers, and business partners. The risk of computer viruses,[1] however, has prompted the IRS to screen for questionable incoming emails, issue a personal use policy[2] on what an employee can and cannot do with email, and conduct awareness training to all employees on the importance of complying with the email use policy. While these efforts established a good foundation for email security, employees are not following the IRS' personal email use policy. In addition, the IRS has unsecured and

Employees are not following the IRS email use policy, and unsecured and unauthorized email servers are putting the internal network at risk.

[1] A computer virus is a piece of programming code that is buried in an existing program and, when executed by the victim, can cause some unexpected and undesirable events. One of the fastest spreading computer viruses was the Love Letter virus, which was sent via email with "I LOVE YOU" in the subject field. This virus replicated itself to everyone in the user's Microsoft Outlook address book, then destroyed local files.
[2] *IRS Policy on Limited Personal Use of Government Information Technology Equipment/Resources*, dated May 3, 2002.

unauthorized email servers[3] on its computer network. As a result, the IRS' internal network, its computers, and the data maintained on the network could be at risk of being compromised, destroyed, or shutdown.

- IRS employees are violating provisions of the personal use policy with their email usage. Specifically, we found inappropriate email messages in 74 percent of the employee mailboxes reviewed. These inappropriate email messages contained chain letters, jokes, offensive content, and sexually explicit content.

  We found 71 (74 percent) of 96 employees had in their electronic mailboxes email messages that violated the IRS' personal use policy.

  The IRS' personal use policy protects the organization from employee actions that might harm or bring unnecessary risk to the organization. For example, hackers have designed email messages containing computer viruses to entice recipients to open them because of their interesting subject lines. Opening these types of emails can activate the computer virus, which in turn could destroy data on computers, enable the hacker to gain unauthorized access to the computer and any sensitive information stored on the computer, and disrupt email and computer operations. While the IRS has conducted awareness presentations and distributed communications to encourage employees to comply with its personal use policy, it does not effectively monitor the email of its employees to ensure compliance with the policy.

- Email servers, like any other computer component, can be vulnerable to computer attacks (e.g., denials of service[4] or buffer overflows[5]) and need to be properly secured and maintained. The IRS maintains 228 authorized email servers to support its email operations. To evaluate the security over email servers, we selected a judgmental sample of 28 email servers and found 687 security vulnerabilities on all 28 servers. People can exploit security vulnerabilities to shut down the servers and disrupt email service or to use the servers to access or attack other computers in the network, which could disrupt other critical operations in the IRS.

In addition, the IRS should limit the number of email servers needed for its email operations to the minimum needed. Aside from the 228 email servers cited above, we identified an additional

[3] An email server is a computer that receives email messages and stores messages in the recipient's electronic mailbox on the computer.
[4] Denial of service attacks inundate a computer system or network with traffic that overloads the system resources, causing them to cease operations or lose network connectivity.
[5] Buffer overflows occur when a user inputs unexpected data to predefined fields that a program is not designed to handle. This situation can cause the program to run supplemental instructions by the user or to cease operation.

4,913 Internet Protocol[6] addresses with devices/servers that have been configured to operate as unauthorized email servers. Any email received through unauthorized email servers would circumvent the security screening established to identify malicious software. If the email contains a computer virus, it could infect the computer as well as the computer network. To evaluate the security of these servers, we selected a sample of 30 and found 363 security vulnerabilities on all 30 computers.

Security vulnerabilities can be exploited to shut down the server and disrupt all other functions of these servers, or use the server to access or attack other computers in the network, which could disrupt other critical operations in the IRS. The majority of the security vulnerabilities on the email servers cited above occurred because system administrators had not installed current security patches[7] to the email servers.

Recommendations

The Chief, Mission Assurance and Security Services, should continue to emphasize the risks associated with inappropriate email use and consider implementing a program of monitoring email message content, which could subsequently increase the number of employees disciplined for abusing their email privileges. The Chief Information Officer should ensure existing procedures are followed to install security updates and patches on all email servers and hold system administrators accountable for ensuring only authorized computers are enabled to perform as email servers.

Response

IRS management agreed with all four of our recommendations. The Chief, Mission Assurance and Security Services, will consider a program to monitor email message content and will also add reminders to existing security awareness training that disciplinary actions have been and will be taken against employees for email abuse. In addition, the Chief Information Officer will hold system administrators accountable for ensuring only authorized computers are enabled to perform as email servers and existing procedures are followed to install security updates and patches on all email servers. Management's complete response to the draft report is included as Appendix IV.

[6] An Internet Protocol address is a unique identifier that devices such as routers, computers, servers, and printers use to identify and communicate with each other on a computer network. The 4,913 Internet Protocol addresses were connected to systems configured to route email.

[7] A patch is a fix to a program as a result of a design flaw in the program. Patches must be installed or applied to the applicable computer to correct the flaw.

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

Table of Contents

Abbreviations

Email	Electronic mail
IRS	Internal Revenue Service

Background

Electronic mail (email) is a form of electronic messaging and is a widely used method of transporting messages across the Internet. The Internal Revenue Service (IRS) relies on email as a method of communication within the organization as well as with external sources for business purposes. Email often replaces memoranda, meetings, and telephone conversations.

Email, however, also presents one of the highest security risks to computer networks. For example, most computer viruses are presently spread through email attachments. A computer virus is a piece of programming code that is buried in an existing program or file and, when executed by the victim, can cause some unexpected and undesirable events. Computer viruses can destroy data on computers, disrupt computer operations, and degrade network performance.[1] As such, it is critical to maintain controls over email use as well as the computer hardware and software installed to support email operations.

In November 2000, we reported there was strong evidence that IRS employee use of email for nonbusiness purposes was significant.[2] In May 2002, given the rapidly expanding use of the Internet and email as today's primary sources of information and personal communication, the IRS implemented a limited personal use policy for the Internet, email, and other equipment and resources.[3] The IRS policy cautions employees to conduct themselves professionally in the workplace and to refrain from using Federal Government information technology equipment and resources for activities that are inappropriate based on established standards of conduct. The IRS considers email as inappropriate if it contains large, nonbusiness file attachments; chain letters; jokes; material that is offensive to other employees; or sexually oriented material. Email pertaining to illegal activities and other prohibited outside activities, such as running a business, fundraising, or restricted political activity, is also considered inappropriate.

As another means to protect itself from incoming emails, the IRS uses software to screen for viruses and other malicious programs that may be hidden in email messages entering the IRS network via the Internet. In addition, it has implemented technical controls to protect its email servers from potential email threats. An email server is a computer that receives email and stores it in the recipient's electronic mailbox. To access the mailbox and read the email, a recipient

[1] One of the fastest spreading computer viruses was the Love Letter virus, which was sent via email with "I LOVE YOU" in the subject field. This virus replicated itself to everyone in the user's Microsoft Outlook address book, then destroyed local files.
[2] *Management Should Take Action to Address Employees' Personal Use of Email* (Reference Number 2001-20-017, dated November 2000).
[3] *IRS Policy on Limited Personal Use of Government Information Technology Equipment/Resources*, dated May 3, 2002.

must enter a logon name and a password. A large organization, such as the IRS, can use many email servers to support its users.

This review was performed at the IRS National Headquarters in Washington, D.C., in the Office of the Chief Information Officer and the Chief, Mission Assurance and Security Services, during the period August 2005 through February 2006. 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.

Results of Review

Employees Are Not Following the Personal Use Policy

Security software used by the IRS prevents many inappropriate messages from entering the IRS network via the Internet. The IRS, however, cannot rely solely on this software. An email virus attack can spread worldwide in minutes, but it may take hours or days for antivirus software vendors to analyze, create, and distribute virus definition updates to protect systems against potential computer virus attacks. In addition to using security software, the IRS has conducted awareness presentations and distributed communications to encourage employees to comply with its email policy. Examples of these awareness efforts include the all-employee annual computer security training modules and periodic communications via email (e.g., the IRS Headlines newsletter).

To determine whether IRS employees were complying with the IRS' personal use policy, we selected a statistical sample of 96 employees from the IRS' list of email addresses and reviewed 46,551 emails received and sent by these employees during June through August 2005. We found 2,576 messages in 71 (74 percent) of the 96 employee mailboxes that violated the IRS' personal use policy. These employees had from 1 to 288 inappropriate emails in their mailboxes. Specifically, we found the following types of inappropriate emails:

We found e-mail messages that violated the IRS' personal use policy in the electronic mailboxes of 71 (74 percent) of 96 employees.

- Chain letters, jokes, and/or pictures accounted for 76 percent of the inappropriate emails. The content is often considered harmless on its own; however, it is well known that these messages present a security threat by being common carriers of malicious software.[4]
- Emails containing content considered offensive according to IRS guidelines accounted for 20 percent of the inappropriate emails. These emails contained hate speech and material that ridiculed others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Emails containing sexually oriented content, prohibited activities, and/or large files accounted for the remaining 4 percent of the inappropriate messages. Prohibited activities include activities conducted for commercial purposes, in support of for-profit activities, or in support of other outside employment.

[4] Malicious software is designed to infiltrate or damage a computer system, without the owner's consent. It includes computer viruses, spyware, and adware.

Figure 1 summarizes these email policy violations by type.

Figure 1: Email Policy Violations by Type

Chain Letters	1,953
Offensive Content	528
Sexually Oriented Content	55
Prohibited Activities	22
Large Files (graphics, video, sound, etc.)	18
TOTAL	**2,576**

Source: Our analysis of a sample of IRS employees' email messages.

The large number of inappropriate emails places the IRS network at risk. For example, malicious software could be attached to these emails that could destroy data on the computer, enable unauthorized persons to access sensitive information, and disrupt computer operations by causing a denial of service attack.[5]

In addition to the security risks, the performance and efficiency of the IRS' computing network is degraded by the number and size of inappropriate email messages. Many of the sampled messages contained graphics, sound, video, and/or animations that significantly increased the sizes of the files. Inclusion of these unnecessary features in an email message often increases the message's size from 10 to 50 times the size of a normal text message, causing the system to operate slower and less efficiently, and creates the need for additional storage capacity that can be costly.

Offensive and inappropriate content in messages can also damage employee relationships and lead to adverse personnel actions or potential lawsuits. When forwarded to outside recipients, these messages could also invite high-profile media attention, damaging the IRS' reputation.

The IRS' personal use policy protects the organization from employee actions that might harm or bring unnecessary risk to the organization. For example, hackers will craft email messages, which contain malicious software, designed to entice recipients to open them because of their interesting subject lines. Opening these types of emails could activate the malicious software, which in turn could destroy data on computers, enable unauthorized persons access to sensitive information, and disrupt computer operations.

[5] Denial of service attacks inundate a computer system or network with traffic that overloads the system resources, causing them to cease operations or lose network connectivity.

The IRS has not effectively monitored the email of its employees to ensure compliance with the policy and has taken relatively few disciplinary actions. For Fiscal Years 2003 through 2005, the IRS disciplined only 283 employees for abuse of email privileges. Of the 283 employees, 193 received written or oral counseling; 86 received formal disciplinary actions including admonishments, reprimands, suspensions, and removal; and 4 resigned. One additional case was referred to the Treasury Inspector General for Tax Administration Office of Investigations.

Recommendations

The Chief, Mission Assurance and Security Services, should:

Recommendation 1: Continue to emphasize the risks associated with inappropriate email use. If reminders that disciplinary actions have been taken against employees for email abuse are added to existing security awareness training, the number of violations may be reduced.

> ***Management's Response:*** The IRS agreed with this recommendation and the Chief, Mission Assurance and Security Services, will ensure inclusion of reminders that disciplinary actions have been and will be taken against employees for email abuse in the next update to the IRS' annual security awareness training.

Recommendation 2: Consider implementing a program of monitoring email message content, which could subsequently increase the number of employees disciplined for abusing their email privileges. This approach will require a commitment of additional resources. However, considering the risks of subjecting the IRS network to malicious software, we believe this commitment is necessary.

> ***Management's Response:*** The IRS agreed with this recommendation and the Chief, Mission Assurance and Security Services, will review the IRS policy on email content monitoring and make a policy recommendation concerning a content monitoring program.

Unsecured and Unauthorized Email Servers Are Putting the Internal Network at Risk

Email servers, like any other computer component, can be vulnerable to many different types of attacks, such as denials of service or buffer overflows,[6] that can lead to the compromise of a single server and even the entire network. The IRS could suffer unauthorized accesses to sensitive information and disruptions of computer operations. To reduce these risks, the IRS must ensure the email servers are configured properly and limit the number of email servers to the minimum needed to continue uninterrupted operations.

[6] Buffer overflows occur when a user inputs unexpected data to pre-defined fields that a program is not designed to handle. This situation can cause the program to run supplemental instructions by the user or to cease operation.

Authorized email servers contain security vulnerabilities

The IRS provided us with a list of 228 authorized email servers. We selected a judgmental sample of 28 of the authorized email servers and performed vulnerability scans using the Nessus[7] security software. Our tests identified 687 security vulnerabilities. Of these, 250 (36 percent) were identified as high risk.[8] The other 437 security vulnerabilities were identified as medium and low risk.[9] Security vulnerabilities were found on all 28 servers.

The majority of the security vulnerabilities occurred because system administrators had not installed current security updates and patches.[10] Untimely installation of patches to existing email servers increases the risk that the systems could be disrupted and vulnerable to new attacks.

All of the existing email servers were replaced during our review, as the IRS migrated all of its email servers to Microsoft Exchange 2003. This migration, begun in August 2005, was completed in April 2006. We scanned 16 Microsoft Exchange 2003 email servers, as of December 2005, and found only minor security vulnerabilities. However, these servers will be subject to the same weaknesses found on the servers that were replaced if system administrators are not diligent in installing security updates and patches as required.

Unnecessary and unauthorized email servers existed on the IRS network

We scanned the entire IRS internal network to identify any computer configured to operate as an email server. In addition to the 228 computers the IRS listed as "authorized" email servers, our scan identified 4,913 Internet Protocol[11] addresses with devices/servers that have been configured to operate as unauthorized email servers. Any emails received by unauthorized servers from outside the IRS network system circumvent the security software installed to screen for malicious software, thus increasing the risk the IRS could suffer unauthorized accesses to sensitive information and disruptions of computer operations unnecessarily. These unauthorized

[7] Nessus is a vulnerability scanning program that identifies security vulnerabilities of the computer on which the program is run.
[8] High-risk vulnerabilities are those that are well known to hackers, are easily exploitable, and have the potential to cause significant damage (e.g., allow an unauthorized person to operate as the root user, giving him or her total access and control of the computer).
[9] Medium-risk vulnerabilities are those that result in a security hole that can lead to privilege escalation; however, an attacker needs additional information or tools to exploit the vulnerability. Low-risk vulnerabilities can provide information to an attacker, but the vulnerability is not a threat in itself.
[10] A patch is a fix to a program as a result of a design flaw in the program. Patches must be installed or applied to the applicable computer to correct the flaw.
[11] An Internet Protocol address is a unique identifier that devices such as routers, computers, servers, and printers use in order to identify and communicate with each other on a computer network. The 4,913 Internet Protocol addresses we identified were connected to systems configured to route email.

servers could also be used to send fictitious email that looks as if it came from a legitimate user and as a means to send spam[12] mail.

From a judgmental sample of 30 of the 4,913 unauthorized devices/servers, we identified 363 security vulnerabilities (on all 30 computers) in the email server applications and the operating systems on which the email applications run. Of these, 149 (41 percent) were identified as high-risk vulnerabilities. The other 214 security vulnerabilities were identified as medium or low risk. The high-risk security vulnerabilities could cause a denial of service, cause buffer overflows that could produce a program crash or erroneous results, or allow unauthorized persons to have access to the computer and possibly execute commands as if the user were the system administrator.

Some portion of the 4,913 unauthorized email servers may be legitimate email servers without being classified as such on the IRS inventory. However, we believe most of the computers were likely installed by the IRS with the default email capability set by the vendor of the operating system. The IRS configuration guide requires system administrators to suppress this capability when installing most operating systems, unless it is specifically needed. Due to the large number of unauthorized email servers identified, we believe system administrators did not comply with these requirements. In addition, the IRS currently does not scan its network to identify and close unauthorized email servers.

Recommendations

The Chief Information Officer should:

Recommendation 3: Ensure existing procedures are followed to install security updates and patches on all email servers. Periodic scans should be conducted to determine whether the updates and patches have been installed.

> ***Management's Response:*** The IRS agreed with this recommendation and the Director, Information Technology Infrastructure, in the Enterprise Operations organization, will ensure local administrators run a program against all email servers that will report any deficiencies in patches and security updates. To ensure all email servers are addressed, the Director, Information Technology Infrastructure, will also work with IRS Chief Counsel and Criminal Investigation functions to help them establish procedures to install security updates and procedures.

Recommendation 4: Hold system administrators accountable for ensuring only authorized computers are enabled to perform as email servers. Periodic scans should be conducted to identify unauthorized servers and applications.

[12] Spam mail is unsolicited email sent indiscriminately to individuals, businesses, and multiple mailing lists; it is often referred to as junk email.

Management's Response: The IRS agreed with this recommendation and the Assistant Chief Information Officer, Enterprise Operations, will review servers to determine their status and identify any unauthorized email servers. If an email server is not authorized, the capability will be disabled unless a business case is approved using a waiver.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS email system was being used properly by employees and was secured by system administrators. Specifically, we:

I. Determined whether employees were complying with the *IRS Policy on Limited Personal Use of Government Information Technology Equipment/Resources* (personal use policy) dated May 3, 2002, regarding email.

   A. Reviewed the personal use policy as it relates to email and determined whether IRS employees were aware of existing guidance and policy by reviewing the training, procedures, and policies provided to employees on the use of email.

   B. Determined the number of adverse actions taken against IRS employees for violating email guidance and policy for Fiscal Years 2003 through 2005.

   C. Selected a random sample of 96 mailboxes from the IRS' Global Address List in Outlook. As of August 1, 2005, the Global Address List had approximately 87,000 users. We selected a statistical (attribute) sample using a 95 percent confidence level, an expected error rate of 50 percent, and a precision of $\pm$10 percent.

   D. Reviewed the sample of 96 mailboxes for messages received and sent during June through August 2005 to determine whether IRS employees were using email in compliance with the IRS' personal use policy.

II. Determined whether the IRS implemented adequate controls to ensure the email system was secure and malicious content was not delivered to the end user.

   A. Determine whether the email servers were configured securely.

      1. Obtained from IRS management a list of 228 authorized Secure Enterprise Messaging Systems email servers, including those mail servers that support the IRS Office of Chief Counsel.

      2. Conducted a Network MAPper[1] scan of the IRS network to identify computers with open ports indicating the potential that an email server was installed on those computers.

[1] This is free security scanner software that can identify certain attributes of the computer against which it is run. These attributes include the operating system and version being used, the ports that are open, and the services being offered.

3. Reviewed for vulnerabilities a judgmental sample of 30 email servers that were not a part of the 228 authorized email servers identified in Step II.A.1. Our port scanning identified 4,913 computers that were not included in the list of authorized email servers. We used a judgmental sample because we did not plan to project the results.
4. Performed security testing on a judgmental sample of 28 of the 228 authorized Secure Enterprise Messaging System mail servers that had not migrated to Microsoft Exchange 2003.
    a. Used the Nessus vulnerability scanner to identify potential vulnerabilities on the selected servers.
    b. Determined whether all operating system and application patches had been installed or mitigating controls had been implemented.
5. Performed security testing on a judgmental sample of 30 email servers that were upgraded or replaced during the Microsoft Exchange 2003 migration. We used automated tools such as the Nessus vulnerability scanner and the Microsoft Baseline Security Analyzer[2] to identify potential vulnerabilities (including missing operating system and application patches) in the operating system and mail application configurations.

B. Determined whether the IRS actively scanned incoming email for malicious content (e.g., email viruses).
    1. Reviewed the rules used to identify malicious content and what types of attachments are allowed.
    2. Determined how often the rules are modified and how often the scanner or antivirus software is updated.
    3. Reviewed the process by which spam[3] and other bulk email is handled.

C. Determined whether the IRS provided its email system administrators sufficient and ongoing training on the email server applications being used by reviewing the training records over the last 2 fiscal years for the email administrators responsible for the authorized email servers.

[2] This is a Microsoft Corporation tool designed to determine the security state of a computer running the Microsoft operating system and to detect common security misconfigurations and missing security updates.
[3] Spam mail is unsolicited email sent indiscriminately to individuals, businesses, and multiple mailing lists; it is often referred to as junk email.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Acting Director
Thomas Polsfoot, Audit Manager
Dan Ardeleano, Senior Auditor
David Brown, Senior Auditor
George Franklin, Senior Auditor
Larry Reimer, Senior Auditor
Esther Wilson, 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 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 Management Controls OS:CFO:AR:M
Audit Liaisons:
- Chief Information Officer OS:CIO
- Chief, Mission Assurance and Security Services OS:MA

Appendix IV

Management's Response to Draft Report

CHIEF INFORMATION OFFICER

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

RECEIVED
JUL 03 2006

JUL 03 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks (Audit # 200520032) (i-trak #2006-13019)

Thank you for the opportunity to review the subject report and respond to the recommendations. We have carefully reviewed the report and agree that the recommendations have merit and require corrective action by the Internal Revenue Service (IRS).

As noted in your report, Mission Assurance and Security Services (MA&SS) will consider implementing a program to monitor email message content. MA&SS will also add reminders to existing security awareness training that disciplinary action has been and will be taken against employees for email abuse.

In addition, the Chief Information Officer will hold system administrators accountable for ensuring that only authorized computers are enabled to perform as email servers and that existing procedures are followed to install security updates and patches on all email servers. We will also conduct periodic scans to determine whether these updates and patches have been installed as well as to identify any unauthorized servers and applications.

Please note that the IRS configures numerous servers with multiple IP addresses. For the report to be accurate, the finding should reflect that 4,913 unauthorized IP addresses, not servers or computers, are configured to perform mail services.

We are committed to improving the administration and security of the IRS email servers and have worked closely with Daniel Galik, Chief, Mission Assurance and Security Services, and members of his staff, in developing this management response. Our responses to the recommendations in this report are attached.

If you have questions, please call me at (202) 622-6800. Members of your staff may also contact Judith Mills, Director, Program Oversight Office, at (202) 283-4915.

Attachment

Attachment

Draft Report – Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks (Audit # 200520032)

RECOMMENDATION #1: The Chief, Mission Assurance and Security Services (MA&SS) should continue to emphasize the risks associated with inappropriate email use. If reminders that disciplinary action has been taken against employees for email abuse are added to existing security awareness training, the number of violations may be reduced.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief, MA&SS will ensure inclusion of reminders that disciplinary action has been and will be taken against employees for email abuse in the next update to the annual security awareness training.

IMPLEMENTATION DATE: July 15, 2007

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: MA&SS will monitor the training calendar to ensure the information is included in the next data call cycle in Spring 2007.

RECOMMENDATION #2: The Chief, MA&SS should consider implementing a program to monitor email message content, which could subsequently increase the number of employees disciplined for abusing their email privileges. This approach will require a commitment of additional resources. However, considering the risks of subjecting the IRS network to malicious software, we believe this commitment is necessary.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief, MA&SS will review the IRS policy on email content monitoring and make a policy recommendation concerning a content monitoring program.

IMPLEMENTATION DATE: May 15, 2007

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: The Chief, MA&SS will monitor the development of a policy recommendation through standing weekly executive direct reports meetings.

RECOMMENDATION #3: The Chief Information Officer should ensure existing procedures are followed to install security updates and patches on all email

1

Attachment

Draft Report – Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks (Audit # 200520032)

servers. Periodic scans should be conducted to determine whether the updates and patches have been installed.

CORRECTIVE ACTION #3a: The IRS agrees with this recommendation. The Director, IT Infrastructure in Enterprise Operations will approve and require the addition of the global security group, DS\MITS Server Standards, to the local administrator group on Secure Enterprise Messaging System (SEMS) email servers owned by this Director. Administrators within this global security group will run a script against the SEMS email servers that will report any deficiencies in patches and security updates. Server Standards will provide the results of the audit to the Director, IT Infrastructure for correction of deficiencies if applicable. If any deficiencies are found, the Director, IT Infrastructure will ensure that these deficiencies are resolved within four (4) business days of receipt of notification. The Director, IT Infrastructure or designee will provide confirmation to Server Standards upon completion of corrective actions. Within five (5) business days of confirmation, Server Standards will run a follow-up scan on SEMS servers to ensure corrective actions have been accomplished.

IMPLEMENTATION DATE: November 1, 2006

RESPONSIBLE OFFICIAL: ACIO, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The SEMS manager will ensure that the actions are implemented.

CORRECTIVE ACTION 3b: In order to ensure all email servers are addressed, the Director, IT Infrastructure will also work with Counsel and Criminal Investigation (CI) to help them establish a set of procedures to install security updates and patches for their email servers.

IMPLEMENTATION DATE: November 1, 2006

RESPONSIBLE OFFICIAL: Director, IT Infrastructure

CORRECTIVE ACTION MONITORING PLAN: The SEMS manager will ensure that the actions are implemented.

RECOMMENDATION #4: The Chief Information Officer should hold system administrators accountable for ensuring that only authorized computers are enabled to perform as email servers. Periodic scans should be conducted to identify unauthorized servers and applications.

2

Attachment

Draft Report – Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks (Audit # 200520032)

CORRECTIVE ACTION: The IRS agrees with this recommendation. The ACIO, Enterprise Operations will review servers to determine their status and identify any unauthorized email servers. If an email server is not authorized, the capability will be disabled unless a qualifying business case is approved via a waiver. The ACIO, Enterprise Operations will issue a policy and

procedures to MITS and the business owners so their system administrators can set the proper security settings to comply with this policy. We have developed a table of actions for system administrators and will remind them of their obligation to monitor the systems and to be accountable for the corrective actions. Quarterly scans of active service ports within the IRS network are currently being performed. These scans will be evaluated and updated as necessary to ensure scans are able to identify unauthorized servers and applications.

IMPLEMENTATION DATE: August 1, 2007

RESPONSIBLE OFFICIAL: ACIO, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: Corrective action status will be reported weekly to oversight coordinators during Enterprise Operations' TIGTA meetings.

3