Sensitive Data Sent Via Email Is Adequately Protected, but Controls Could Be Streamlined

February 2005

Reference Number: 2005-20-038

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 22, 2005

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Sensitive Data Sent Via Email Is Adequately Protected, but Controls Could Be Streamlined (Audit # 200420022)

This report presents the results of our review of the Internal Revenue Service's (IRS) controls to protect sensitive data sent via email. The IRS routinely works with sensitive but unclassified data such as taxpayers' personal financial data and employees' data. Most managers and employees have access to email and can send sensitive data to other employees to expedite their work. Including sensitive data in email poses certain risks. Specifically, email, if not properly encrypted, can be intercepted by unauthorized persons, and employees can inadvertently disclose sensitive data by sending email to the wrong recipient. The overall objective of this review was to determine whether the IRS is adequately protecting sensitive data sent via email.

In summary, the IRS has controls in place to adequately protect sensitive data sent via email. The IRS uses features available on its email system to automatically encrypt emails. Encryption is a method of "scrambling" text or data so that it is unreadable. Software on each employee's computer encrypts data prior to moving the data across network lines. Emails transmitted from one IRS building to another IRS building are encrypted at an even higher level than emails transmitted within an IRS building.

Emails forwarded outside the IRS network (e.g., to taxpayers or employees' home computers) are not encrypted. However, we found no instances in our tests of sensitive emails being forwarded outside the IRS network.

The IRS established its Secure Messaging program in June 2002 to ensure that emails containing sensitive data sent within IRS buildings were encrypted at the same level as emails sent between IRS buildings. Secure Messaging also keeps messages encrypted while stored on servers, creates employee awareness to protect sensitive data, and

gives the IRS experience that may be beneficial if similar technology is ever used for broader purposes. However, Secure Messaging has several disadvantages. Primarily, it is difficult for management to enforce its use.

When the IRS implemented Secure Messaging in June 2002, the goal was to have 100 percent of all employees enrolled in the program by September 30, 2002. However, as of September 2004, 2 years into the program, IRS records indicated that only 76 percent of the nearly 82,000 email mailboxes had been enrolled. Since both the sender and receiver of an email must be enrolled in Secure Messaging for it to work, its effectiveness has been limited. Additionally, IRS employees, even those enrolled in the Secure Messaging program, are not using it consistently. In our sample, 43 percent of the mailboxes contained sensitive data that had not been encrypted with Secure Messaging as required.

Secure Messaging also requires additional expenditures. It increases the size of email messages which places more demands on the IRS telecommunications system and computer storage capabilities. In addition to the $350,000 spent to start up the original Secure Messaging program, the IRS is incurring ongoing costs to administer it. The program requires dedicated servers and 5 part-time employees at a cost of $156,000 per year to manage the hardware and software.

At your request, we evaluated Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, entitled “Policy for Common Identification Standard for Federal Employees and Contractors,” and determined that this Directive has no impact on Secure Messaging.

We recommended the Chief Information Officer (CIO) coordinate with business unit owners to reevaluate and weigh the costs and benefits of continuing the Secure Messaging program. If the CIO and the business unit owners determine that the program should continue, they should ensure all IRS employees who send sensitive data via email are enrolled in the Secure Messaging program and comply with its procedures. In addition to continuing awareness training efforts, first-line managers should periodically review employees’ use of Secure Messaging to ensure compliance.

Management’s Response: The CIO agreed with two of the three recommendations in this report. The CIO will promote employee awareness of the Secure Messaging program through the Modernization and Information Technology Services (MITS) organization’s website and other communication channels as needed. The Mission Assurance and Security Services (MA&SS) organization will incorporate Secure Messaging within the annual online computer security awareness training required for all employees. The MA&SS and MITS organizations plan to issue a joint memo mandating the enrollment of all employees in the Secure Messaging program, and the MITS organization will work with the business units to develop a cost-effective way of assessing compliance. The CIO did not agree to coordinate with business owners to reevaluate and weigh the costs and benefits of the Secure Messaging program as we recommended. Citing HSPD 12, dated August 27, 2004, entitled “Policy for Common Identification Standard for Federal Employees and Contractors,” the CIO will continue

using Secure Messaging as a key component in the IRS' transition to implement Public Key Infrastructure as a logical access control. The CIO also questioned our sampling methodology. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We believe the conclusions and recommendations in this report are valid. Based on our review of HSPD 12 and interviews with Federal Government experts on the subject, we believe HSPD 12 is not relevant to Secure Messaging. Regarding our sampling methodology, we selected a random sample of 60 mailboxes and reviewed approximately 21,000 emails in our review and reached conclusions based on that analysis. Our sample was clearly large enough to support our conclusion that IRS employees are not complying with Secure Messaging procedures. A statistical sample was not necessary because we did not intend to project our results to the entire population of IRS emails. We made the recommendation to evaluate costs and benefits because we believe the IRS could save costs and reduce the impact on managers and employees by not requiring Secure Messaging. While we still believe our recommendation is worthwhile, we do not intend to elevate our disagreement concerning it to the Department of the Treasury for resolution.

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

Sensitive Data Sent Via Email Is Adequately Protected, but Controls Could Be Streamlined

Background

The Internal Revenue Service (IRS) routinely works with sensitive but unclassified (SBU) data such as taxpayers' personal financial data, law enforcement information, and employees' data. Most managers and employees have access to email and can send sensitive data to other employees to expedite their work. Including sensitive data in email poses certain risks. Specifically, email, if not properly encrypted, can be intercepted by unauthorized persons, and employees can inadvertently disclose sensitive data by sending emails to the wrong recipient.

The National Institute of Standards and Technology (NIST)[1] publication *Guidelines on Electronic Mail Security* (NIST SP 800-45) recommends specific levels of encryption for Federal Government organizations to protect email during the transmission of messages. The NIST guidelines also recommend encrypted messages be stored in their encrypted format. Treasury Directive 85-01, dated June 12, 2003, directs all bureaus to provide appropriate security for their email systems in accordance with NIST SP 800-45 guidance.

The IRS established the Secure Messaging program in June 2002 to address the NIST guidelines and its concerns with sending sensitive data via email. Secure Messaging allows users to encrypt messages so only recipients who have been granted the secure messaging capability can decrypt and read the message and any attachments.

At the request of the IRS' Chief Information Officer (CIO), we evaluated Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, entitled "Policy for Common Identification Standard for Federal Employees and Contractors" to determine if it had an impact on Secure Messaging. We also reviewed the draft Federal Information Processing Standards Publication 201, entitled "Personal Identity Verification (PIV) for Federal Employees and Contractors," and attended a public forum on HSPD 12.

[1] The NIST is a non-regulatory Federal agency within the United States Commerce Department's Technology Administration. It promotes the United States economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure.

Our analysis determined that this Directive has no impact on Secure Messaging.

This review was performed in the Office of the CIO at the IRS National Headquarters in Washington, D.C., during the period April through September 2004. 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.

Controls Are in Place to Protect Sensitive Data Sent Via Email

Data sent from employee to employee is protected across the IRS network

The IRS uses features available on its email system to automatically encrypt emails. Encryption is a method of "scrambling" text or data so that it is unreadable. Software on each employee's computer encrypts data prior to moving the data across network lines. The text or data is then decrypted, or unscrambled, on the receiver's computer so it is again readable. Emails sent between IRS buildings are encrypted at an even higher level than emails sent within an IRS building.

We found no evidence that employees were sending emails containing SBU data outside the IRS

Emails sent outside the IRS wide area network (e.g., to taxpayers or employees' home computers) are not encrypted and, as a result, the IRS prohibits this practice. We judgmentally selected mailboxes of 60 employees who would likely work with sensitive data. To accomplish this, we selected employees that work in five of the IRS' business units: the Appeals function, Agency-Wide Shared Services, Small Business/Self-Employed Division, Large and Mid-Size Business Division, and Tax Exempt and Government Entities Division. In our review of emails sent from these mailboxes over a 14-week period from April 1, 2004, to July 14, 2004, we did not identify any emails containing SBU data that were sent outside the IRS network.

The Encryption of Emails Could Be Streamlined

The IRS established its Secure Messaging program in June 2002 to enhance the encryption of emails containing sensitive data. To successfully use Secure Messaging, both the sender and receiver must enroll in the program. To

enroll, users access a web site so security personnel can ensure the user's computer meets certain security configurations.

Secure Messaging uses Public Key Infrastructure (PKI) technology to encrypt emails. PKI technology protects messages with a combination of public and private "keys" which allows users to encrypt and decrypt the messages. Both sender and receiver must be listed on the IRS' list of email addresses to enroll in Secure Messaging.

To encrypt a message, the sender must select the recipient's name from the IRS' list of email addresses and also select the Secure Messaging option when sending the message. To decrypt the message, the recipient must enter a previously chosen password that can be used to open all of their emails encrypted with Secure Messaging.

Secure Messaging does provide the IRS with certain enhancements. For example:

- The use of Secure Messaging creates an awareness of the need to protect sensitive data when using email.
- Secure Messaging provides the capability to provide the same level of encryption for emails sent within an IRS building as emails sent between IRS buildings. This encryption is effective even if the network encryption fails.
- Secure Messaging keeps messages encrypted while stored on email servers and user workstations. Without Secure Messaging, emails are encrypted only during transmission.
- The Department of the Treasury is exploring potential uses of PKI technology. Using PKI technology in the Secure Messaging program could give the IRS some experience that may be beneficial if PKI technology is ever used for broader purposes.

While Secure Messaging does enhance encryption, it has several disadvantages. Primarily, it is difficult for management to enforce its use.

When the IRS implemented the Secure Messaging program in June 2002, the goal was to have 100 percent of all employees enrolled in Secure Messaging by September 30, 2002. However, as of September 2004, 2 years into the program, IRS records showed that only 62,535 (76 percent) of the 81,913 total email mailboxes were enrolled in the Secure Messaging program.

In addition, management has not ensured employees comply with the requirements to encrypt all emails containing SBU data. Employees are not always using the Secure Messaging encryption process when sending SBU data internally.

We judgmentally selected 60 email mailboxes and reviewed messages that were composed between April 1, 2004, and July 14, 2004. Our sample of 20,983 emails was comprised of 30 employees who were enrolled (12,546 emails) and 30 employees not enrolled (8,437 emails) in the Secure Messaging program.

We identified 183 unencrypted messages containing SBU data in 26 (43 percent) of the 60 mailboxes reviewed. We found that 110 (60 percent) of the 183 unencrypted messages were in non-enrolled users' mailboxes. However, more than half the employees enrolled in Secure Messaging also had unencrypted emails with sensitive data in their mailboxes.

Although the use of Secure Messaging has been mandated by the IRS, managers have not provided sufficient attention to ensure employee compliance. To enforce the use of Secure Messaging, managers would have to periodically review email files on employees' computers to determine if they had used Securing Messaging to encrypt sensitive data. We recognize this effort could be overly burdensome for first-line managers in addition to the other requirements for their time.

Secure Messaging has other disadvantages. For example:

- The added encryption provided by Secure Messaging increases the size of messages. While the impact on a small email message is insignificant, the impact on a large message with attachments can increase the size of the email by 25 to 30 percent.

Consequently, the IRS must use additional network bandwidth for transmission and more storage space on email servers.

- In addition to the $350,000 initially spent to implement the Secure Messaging program, the IRS is incurring ongoing costs to administer it. The program requires dedicated servers and 5 part-time employees costing about $156,000 per year to manage the hardware and software. The IRS could potentially put these funds to better use if Secure Messaging were not continued.

While Secure Messaging provides additional protection when using email, the use of this feature requires substantial management oversight and associated costs. NIST guidance recommends organizations weigh the costs and benefits associated with implementing a sound encryption policy. To our knowledge, the IRS has not reevaluated the need or weighed the costs and benefits for the Secure Messaging program since it was implemented in June 2002.

Recommendations

The CIO should coordinate with business unit owners to:

1. Reevaluate and weigh the costs and benefits of continuing the Secure Messaging program.

Management's Response: The CIO did not agree with this recommendation. The CIO indicated with the issuance of HSPD 12, dated August 27, 2004, entitled "Policy for Common Identification Standard for Federal Employees and Contractors," all Federal Government agencies are mandated to implement PKI as a central component of logical access controls. Since Secure Messaging provides a useful migration path to PKI, it will remain a key component of the IRS' transition activities. The CIO also questioned our sampling methodology.

Office of Audit Comment: We believe the conclusions raised and recommendations in this report are valid. Based on our review of HSPD 12 and interviews with Federal Government experts on the subject, we believe HSPD 12 is not relevant to Secure Messaging. Regarding our sampling methodology, we selected a random sample of 60 mailboxes

and reviewed approximately 21,000 emails in our review and reached conclusions based on that analysis. Our sample was clearly large enough to support our conclusion that IRS employees are not complying with Secure Messaging procedures. A statistical sample was not necessary because we did not intend to project our results to the entire population of IRS emails. We made the recommendation to evaluate costs and benefits because we believe the IRS could save costs and reduce the impact on managers and employees by not requiring Secure Messaging.

If the CIO and business unit owners decide to continue the Secure Messaging program they should:

2. Continue awareness training to encourage all IRS employees who send sensitive data via email to enroll in the Secure Messaging program and comply with its procedures.

Management's Response: The Modernization and Information Technology Services (MITS) organization will continue to promote employee awareness. The Mission Assurance and Security Service (MA&SS) organization will incorporate Secure Messaging with the annual online computer security awareness training required for all employees.

3. Require first-line managers to periodically review employees' use of Secure Messaging to ensure compliance.

Management's Response: The MA&SS and MITS organizations will issue a joint memo mandating the enrollment of all employees in secure messaging. The MITS organization will work with the business units to develop a cost-effective way of assessing compliance.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess whether the Internal Revenue Service (IRS) is adequately protecting sensitive data sent via email. To accomplish this objective, we:

I. Determined whether the use of Secure Messaging was necessary and effective for reducing the risk of sensitive data being intercepted or whether the other levels of encryption used by the IRS were adequate.

- A. We interviewed responsible IRS officials and reviewed policies, laws, and standards applicable to Secure Messaging encrypted email, as well as the network flow of general and sensitive data.
- B. We compared these requirements with the encryption levels documented in the IRS' Certification and Accreditation report, local and wide area network infrastructure, and software specifications.
- C. We determined and illustrated the encryption and decryption points in the data transmission stream.
- D. At the request of the IRS' Chief Information Officer, we evaluated Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, entitled "Policy for Common Identification Standard for Federal Employees and Contractors," reviewed the draft Federal Information Processing Standards Publication 201, entitled "Personal Identity Verification (PIV) for Federal Employees and Contractors," and attended a public forum on HSPD 12 to determine whether it has any impact on Secure Messaging.

II. Determined whether Secure Messaging encryption was applied effectively and consistently to protect sensitive data sent via email.

- A. We identified the total number of IRS employee mailboxes and the number enrolled in the Secure Messaging program.
- B. We determined whether IRS employees were sending sensitive data via email without using the Secure Messaging feature by selecting a judgmental sample. We selected a judgmental sample because we did not intend to project the results to all mailboxes.

We selected mailboxes from specific business units that we believed would have the most likelihood of sending emails with sensitive data. From the IRS' Secure Messaging website, we were able to download all IRS email users both enrolled and not enrolled in Secure Messaging, a total of 82,439 mailboxes. We separated five offices: Appeals, Agency-Wide Shared Services, Small Business/Self-Employed Division, Large and Mid-Size Business Division, and the Tax Exempt and Government Entities Division. These offices accounted for 34,474 mailboxes. We selected a random sample of 30 mailboxes from both the enrolled and not enrolled users in these offices, for a total of 60 sampled mailboxes. We reviewed 20,983 emails sent and received by these employees from April 1, 2004, to July 14, 2004.

III. Determined whether IRS employees were forwarding and/or sending sensitive data via email outside the IRS network, either to taxpayers or their own personal computers, by reviewing the messages from our sample in Step II. B. and IRS logs of messages sent outside the IRS networks.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Thomas Polsfoot, Audit Manager
David Brown, Senior Auditor
George Franklin, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief, Mission Assurance and Security Services OS:MA
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Assurance Programs OS:MA:AP
Director, Business Systems Development OS:CIO:I:B
Director, End User Equipment and Services OS:CIO:I:EU
Director, Enterprise Networks OS:CIO:I:EN
Director, Enterprise Operations Services OS:CIO:I:EO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of 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 the Draft Report

CHIEF INFORMATION OFFICER

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

RECEIVED
FEB 10 2005

February 9, 2005

MEMORANDUM FOR ACTING DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams WTG
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – Sensitive Data Sent Via Email Is Adequately Protected, but Controls Could Be Streamlined – Audit #200420022 (**ECMS # 0501-68ZHU6BL**)

Thank you for the draft audit report on our secure messaging system. We are pleased with the audit teams' conclusion that the Internal Revenue Service (IRS) adequately protects sensitive data sent via email.

We also appreciated receiving the additional information pertaining to the audit teams' sample selection as well as their review of the August 27, 2004 Homeland Security Presidential Directive 12 (HSPD-12) entitled "Policy for Common Identification Standard for Federal Employees and Contractors".

Please note that we do not agree with the auditors' assessment that HSPD-12 has no impact on secure messaging. While this directive does not specifically speak to messaging authentication and signing, it does mandate that all government agencies (including the IRS) migrate to logical access controls based on Public Key Infrastructure (PKI) technology in the near-term. As such, the Modernization and Information Technology Services (MITS) organization will be replacing the IRS' existing secure messaging program with PKI as a foundation for infrastructure authentication. Consequently, we do not concur with the recommendation that the Chief Information Officer should coordinate with business owners to reevaluate and weigh the costs and benefits of continuing the secure messaging program.

Additionally, the audit team judgmentally selected 60 email mailboxes (of which 30 employees were enrolled in the secure messaging program and 30 were not), and reviewed messages that were composed between April 1, 2004 and July 14, 2004. The team identified 183 unencrypted messages containing Sensitive But Unclassified (SBU) data in 26 (or 43 percent) of the 60 mailboxes reviewed. Of these, 110 (or 60 percent) of the 183 unencrypted messages were in non-enrolled users' mailboxes. The IRS generates 11 million email messages per week. As such, the IRS' Statistics of Income

Division determined at least 80,000 messages would need to be reviewed in order to draw a statistically sound decision.

Also, we have been promoting employee awareness of the need to send messages securely, and we plan to continue our awareness campaign in 2005. While MITS does not have jurisdiction to ensure all employees enroll in the secure messaging program and that first-line managers periodically conduct compliance reviews, Mission Assurance and the CIO organization plan to issue a joint memo mandating the enrollment of all employees in secure messaging. MITS will work with the business units to develop a cost effective way of assessing compliance.

We appreciate your continued support as well as the valuable assistance and guidance we receive from your staff. If you have questions, please contact me at (202) 622-6800, or a member of your staff may contact Judy Mills, Acting Director of Program Oversight, at (202) 283-4915.

Attachment

Attachment

Management Response to Draft Audit Report # 200420022 --
Sensitive Data Sent Via Email is Adequately Protected,
But Controls Could be Streamlined

RECOMMENDATION #1: The Chief Information Officer (CIO) should coordinate with business owners to reevaluate and weigh the costs and benefits of continuing the secure messaging program.

MANAGEMENT RESPONSE: While we understand the need to evaluate programs for cost and benefit analysis, the CIO does not agree with this recommendation. With the advent of Homeland Security Presidential Directive 12, all government agencies (including the IRS) are mandated to implement Public Key Infrastructure (PKI) as a central component of logical access controls. The draft audit report states that secure messaging provides a useful migration path for PKI implementations. Hence, secure messaging will remain a key component of our transition activities.

RECOMMENDATION #2: If the Chief Information Officer and business unit owners decide to continue the secure messaging program they should continue awareness training to encourage all IRS employees who send sensitive data via email to enroll in the secure messaging program and comply with its procedures.

CORRECTIVE ACTION #2A: The Modernization and Information Technology Services (MITS) organization will continue to promote employee awareness of secure messaging through the MITS Website and other communications channels as needed. We will follow promotion standards for other secure messaging protocols (e.g., PKI) as they become available.

IMPLEMENTATION DATE: December 20, 2004

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN #2A: Not applicable.

CORRECTIVE ACTION #2B: Mission Assurance and Security Services (MA&SS) will incorporate secure messaging within the all-employee required annual online computer security awareness training.

IMPLEMENTATION DATE: October 1, 2005

RESPONSIBLE OFFICIAL: Chief, Information Technology Security Services (ITSS)

1

Attachment

Management Response to Draft Audit Report # 200420022 --
Sensitive Data Sent Via Email is Adequately Protected,
But Controls Could be Streamlined

CORRECTIVE ACTION MONITORING PLAN #2B: The Chief, ITSS will monitor inclusion of secure messaging within the course updates to the computer security awareness online course design and development plan.

RECOMMENDATION #3: If the Chief Information Officer and business unit owners decide to continue the secure messaging program, they should require first-line managers to periodically review employees' use of secure messaging to ensure compliance.

CORRECTIVE ACTION: The Modernization and Information Technology Services (MITS) organization has issued several messages to the IRS business units encouraging them to ensure that their managers and employees enroll in and use secure messaging. The CIO issued a memo dated September 14, 2000 updating employees on IRS' email security policy. Subsequently, a second memo on secure messaging was issued on June 20, 2002. MITS does not have jurisdiction to ensure all employees enroll in the program and that first-line managers periodically conduct compliance reviews, however, Mission Assurance and MITS plan to issue a joint memo mandating the enrollment of all employees in secure messaging. MITS will work with the business units to develop a cost effective way of assessing compliance.

IMPLEMENTATION DATE: April 1, 2005

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: The Director of End User Equipment and Services will monitor the drafting of a joint Mission Assurance/CIO memo requiring the business units to enroll their employees in secure messaging, and MITS will work with the business units to develop a cost effective method of assessing compliance.