



Treasury Inspector General for Tax Administration Office of Audit

ADDITIONAL SECURITY IS NEEDED FOR THE TAXPAYER SECURE EMAIL PROGRAM

Issued on February 4, 2011

Highlights

Highlights of Report Number: 2011-20-012 to the Internal Revenue Service Chief Technology Officer; Commissioner for Large Business and International Division; Chief of the Office of Appeals; and Director of the Office of Privacy, Information Protection and Data Security.

IMPACT ON TAXPAYERS

Internal Revenue Service (IRS) employees and taxpayers are required to work together to ensure the security of taxpayers' sensitive data transmitted in email messages. If employees and taxpayers do not follow the required security policies, the risks to taxpayers' sensitive data are increased. The data could be intercepted and accessed by unauthorized individuals or inadvertently sent to the wrong recipient.

WHY TIGTA DID THE AUDIT

This audit was initiated because the IRS relaxed its long-standing internal policy prohibiting employees from transmitting Sensitive But Unclassified (SBU) data to taxpayers in emails. The objective of the review was to determine whether IRS controls, policies, and procedures for sensitive email messages to taxpayers adequately protected taxpayers' data, guarded against email threats to the IRS network, and ensured email practices were compliant with Federal regulations.

WHAT TIGTA FOUND

Although some controls, such as the installation of antivirus software on employees' computers, for the Secure Email With Taxpayers program are in place, other security controls were not implemented. The IRS has not implemented an automated control to detect and prevent SBU data in unencrypted emails from being transmitted outside the IRS. In addition, some employees and taxpayers are not encrypting their emails that contain SBU data. These violations of the program were not reported to IRS management. Furthermore, IRS procedures and training lacks adequate guidance for employees to report the violations. In addition, the IRS does not timely correct persistent medium-risk security vulnerabilities detected on email servers.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Large Business and International Division and the Office of Appeals coordinate with the Office of Privacy, Information Protection and Data Security, to develop additional procedures for employees participating in the Secure Email With Taxpayers program to address how, when, and to whom employee and taxpayer secure email violations should be reported; update guides and training materials to include these procedures; amend the Memorandum of Understanding to apprise the taxpayer of the specific risks associated with transmitting unencrypted email with SBU data; and issue a memorandum to all employees advising them of the disciplinary actions that will be taken against employees who violate IRS email policies by sending unencrypted emails to taxpayers who have not signed a Memorandum of Understanding to participate in the program.

TIGTA also recommended that the Associate Chief Information Officer, Cybersecurity, ensure data leakage prevention software is implemented by April 2012, and update the annual Information Systems Security briefing to include the new Secure Email With Taxpayers procedures. Lastly, TIGTA recommended the Associate Chief Information Officer, Enterprise Operations, ensure medium-risk vulnerabilities detected on email servers are appropriately tracked and, if the vulnerabilities cannot be corrected within two months, follow security requirements to post the vulnerabilities to the appropriate Plan of Actions and Milestones.

In their response to the report, IRS officials agreed with six of the recommendations and partially agreed with three. For the three partially agreed recommendations, TIGTA continues to believe that the IRS should fully implement the recommendations.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

<http://www.treas.gov/tigta/auditreports/2011reports/201120012fr.pdf>.

Email Address: TIGTACommunications@tigta.treas.gov

Phone Number: 202-622-6500

Web Site: <http://www.tigta.gov>