Treasury Inspector General for Tax Administration
Office of Audit

THE INTERNAL REVENUE SERVICE DEPLOYED THE MODERNIZED E-FILE SYSTEM WITH KNOWN SECURITY VULNERABILITIES

Issued on December 30, 2008

Highlights

Highlights of Report Number: 2009-20-026 to the Internal Revenue Service Commissioner for the Wage and Investment Division and the Chief Technology Officer.

IMPACT ON TAXPAYERS

The Modernized e-File (MeF) system will provide a single method for filing all Internal Revenue Service (IRS) tax returns, information returns, forms, and schedules via the Internet. The Modernized Tax Return Database (M-TRDB), a component of the MeF system, is the authoritative store of accepted returns and extensions submitted through the MeF system. Security weaknesses in the controls over system access, monitoring of system access, and disaster recovery have continued to exist even though key phases of the MeF system and the M-TRDB have been deployed. As a result, the IRS is jeopardizing the confidentiality, integrity, and availability of an increasing volume of tax information for millions of taxpayers as application phases are put into operation.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's statutory requirements to annually review the adequacy and security of IRS information technology. The overall objective of this review was to determine whether appropriate security controls have been implemented in the MeF system.

WHAT TIGTA FOUND

TIGTA's review of test documents provided by the IRS showed that both the MeF and the M-TRDB were deployed with known security vulnerabilities relating to protection of sensitive data, system access, monitoring of system access, and disaster recovery. These vulnerabilities increase the risks that 1) an unscrupulous person could gain unauthorized access to taxpayer information the IRS processes with little chance of detection and 2) the systems could not be recovered effectively and efficiently during an emergency.

The MeF project office did not prevent and resolve known security vulnerabilities before deployment of the system. The Submission Processing Executive Steering Committee (the Committee), which has final milestone exit approval, 1) did not provide sufficient oversight to ensure that security controls were implemented and 2) signed off unconditionally on MeF system milestones despite the existence of weaknesses repeatedly reported to the Committee. Finally, the Cybersecurity organization recommended, and the MeF system owner accepted, that the system be fully accredited without giving adequate consideration of what TIGTA views as significant security vulnerabilities on the system. In our opinion, the system owner's acceptance of the excessive risks associated with these security vulnerabilities was not reasonable.

WHAT TIGTA RECOMMENDED

TIGTA recommended that 1) the Committee consider all security vulnerabilities that affect the overall security of the MeF system and the M-TRDB before approving milestone exits; 2) the Commissioner, Wage and Investment Division, and the Chief Information Officer provide more emphasis to the MeF project office to both prevent and resolve security vulnerabilities identified during Enterprise Life Cycle processes; and 3) the Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, as the MeF system owner, approve interim authorities to operate when significant security control weaknesses exist in system environments.

In their response to the report, IRS officials agreed with our recommendations. IRS management plans to continue to 1) follow the governance process documented in the Committee charter, which includes the review of all security vulnerabilities, before milestone exits; 2) follow the existing life cycle processes for identifying, confirming, and resolving security vulnerabilities at the different stages, with an increased emphasis in both preventing and resolving security vulnerabilities identified; and 3) operate in accordance with policies and procedures. If and when they find that significant control weaknesses exist in the system environments, they plan to issue an interim authority to operate with the appropriate timelines based on the level of risk.

The corrective actions for the recommendations are focused on continuing to follow or strengthening existing processes. TIGTA believes that the security vulnerabilities were not caused by process deficiencies. Instead, IRS personnel did not fulfill their responsibilities for correcting security vulnerabilities before deployment.

READ THE FULL REPORT

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

http://www.treas.gov/tigta/auditreports/2009reports/200920026fr.pdf.

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