Treasury Inspector General for Tax Administration
Office of Audit

THE INTERNAL REVENUE SERVICE DEPLOYED TWO OF ITS MOST IMPORTANT MODERNIZED SYSTEMS WITH KNOWN SECURITY VULNERABILITIES

Issued on September 24, 2008

Highlights

Highlights of Report Number: 2008-20-163 to the Internal Revenue Service Commissioner for the Wage and Investment Division and the Chief Information Officer.

IMPACT ON TAXPAYERS

The Customer Account Data Engine (CADE) will provide the foundation for managing all taxpayer accounts and will replace existing tax processing systems. The Account Management Services (AMS) will provide faster and improved access by employees to taxpayer account data. Security weaknesses in controls over sensitive data protection, system access, monitoring of system access, and disaster recovery have continued to exist even though key phases of the CADE and the AMS have been deployed. As a result, the Internal Revenue Service (IRS) is jeopardizing the confidentiality, integrity, and availability of an increasing volume of tax information for millions of taxpayers as these systems 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 objective was to determine whether appropriate security controls were implemented in the CADE and the AMS systems.

WHAT TIGTA FOUND

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

TIGTA believes that key organizations did not consider the known security vulnerabilities to be significant, which affected vulnerability resolution and system deployment decisions. Specifically, the CADE and AMS project offices did not prevent and resolve known security vulnerabilities before deployment of the systems. The Customer Service Executive Steering 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 CADE milestones despite the existence of weaknesses repeatedly reported to the Committee. Finally, the Cybersecurity organization recommended–and the system owners accepted–the risks associated with these vulnerabilities by accrediting the systems. TIGTA disagreed with the system owners' acceptance of these security vulnerabilities.

WHAT TIGTA RECOMMENDED

TIGTA recommended that 1) the Customer Service Executive Steering Committee consider all security vulnerabilities that affect the overall security of the CADE and the AMS before approving unconditional milestone exits, 2) the CADE and AMS Project Managers provide more emphasis on preventing and resolving security vulnerabilities identified, and 3) the CADE and AMS system owners approve interim authorities to operate when significant security control weaknesses exist in system environments. In addition, the Associate Chief Information Officer, Cybersecurity, should 4) recommend interim authorities to operate when significant security vulnerabilities exist in system environments and 5) continue efforts to improve the accuracy and completeness of risk information in the security assessment reports.

In their response to the report, IRS officials agreed with our recommendations. The IRS plans to follow the governance process documented in the Customer Service Executive Steering Committee charter and consider all security vulnerabilities for delivery of project security and functionality; follow existing Enterprise Life Cycle processes for identifying, confirming, and resolving security vulnerabilities; strengthen its processes for documenting all Executive Steering Committee meeting minutes; follow its policy to issue interim authorities to operate when significant control weaknesses exist; and modify the certification and accreditation process to include documented concurrence when security weaknesses have been corrected.

The related 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/2008reports/200820163fr.pdf.

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