



Treasury Inspector General for Tax Administration Office of Audit

SIGNIFICANT DELAYS HINDERED EFFORTS TO PROVIDE CONTINUOUS MONITORING OF SECURITY SETTINGS ON COMPUTER WORKSTATIONS

Issued on January 24, 2013

Highlights

Highlights of Report Number: 2013-20-016 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Effective continuous monitoring of computer workstations allows security issues to be identified and mitigated promptly, reducing the likelihood of a security breach. When IRS data and its network are not secured, taxpayer information becomes vulnerable to unauthorized disclosure and theft. Furthermore, security breaches can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquiries. In addition, the IRS collects vast quantities of personal and financial information that can be targeted for identity theft.

WHY TIGTA DID THE AUDIT

This audit was included in TIGTA's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to determine whether the IRS is effectively and efficiently implementing its continuous monitoring tool to monitor security settings on employee workstations and laptop computers.

WHAT TIGTA FOUND

The Treasury Enhanced Security Initiatives project, which includes the continuous monitoring tool for workstation security, will address several computer security weaknesses. The IRS appropriately acquired the project's multiple software components, and the project team completed key documentation during the development process, ensuring that critical issues were identified and addressed. However, the Treasury Enhanced Security Initiatives project has experienced several delays, and the project's oversight board did not take required actions to manage the delays or the associated costs. The IRS was scheduled to deploy the security tools in December 2010 but now plans to complete the deployment in May 2013.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer direct the Cybersecurity and Privacy Governance Board to: 1) review total actual life cycle costs for projects at least quarterly and review variances between actual costs and the originally proposed estimated costs, 2) manage costs by considering the postponement of projects with long-term delays, and 3) escalate ongoing project delays to the higher level Security Services and Privacy Executive Steering Committee.

In their response to the report, IRS officials agreed with TIGTA's recommendations. The IRS plans to review information technology projects' life cycle costs, consider postponing those projects with long-term delays, and escalate delays to the higher level Security Services and Privacy Executive Steering Committee.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2013reports/201320016fr.pdf>