



Treasury Inspector General for Tax Administration Office of Audit

FULL COMPLIANCE WITH TRUSTED INTERNET CONNECTION REQUIREMENTS IS PROGRESSING; HOWEVER, IMPROVEMENTS WOULD STRENGTHEN SECURITY

Issued on September 17, 2013

Highlights

Highlights of Report Number: 2013-20-107 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Trusted Internet Connection (TIC) initiative is one of the Administration's three priorities to improve cybersecurity and the security of Federal information systems. The TIC initiative aims to improve agencies' security posture and incident response capabilities through enhanced monitoring and situational awareness of all external network connections. The IRS has progressed steadily towards implementing TIC requirements; however, additional improvements could strengthen the security posture of its TICs. Security weaknesses within these TICs could expose taxpayer data to unauthorized access or loss.

WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The objective of this audit was to evaluate the IRS's three TICs to ensure that the connections comply with Department of Homeland Security requirements. The Administration expects Federal agencies to achieve 100 percent compliance with TIC requirements by Fiscal Year 2014.

WHAT TIGTA FOUND

Although the IRS has made good progress implementing the TIC requirements, our review revealed areas where improvements could strengthen the security posture of the TICs. For example, the IRS was not logging administrative activity on TIC equipment, had not completed actions to fully implement TIC requirements for a Data Loss Prevention program, did not have sufficient staff with the required security clearance and proper locations for handling classified information, and was not regularly scanning TIC equipment to ensure timely discovery and mitigation of vulnerabilities or misconfigurations.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that the IRS: 1) implements the capture and review of administrator activity on TIC devices; 2) fully implements the selected tool for the Data Loss Prevention program upon successful testing; 3) obtains Top Secret Sensitive Compartmented Information clearances for IRS operational employees who can receive and react to classified information on a 24/7 basis; 4) completes implementation of proper locations for handling classified information at TIC locations; 5) implements vulnerability and configuration management scanning on TIC equipment and mitigates reported findings; and 6) updates all TIC equipment to the most current operating systems approved for use within the IRS.

The IRS agreed with all of TIGTA's recommendations and has planned appropriate corrective actions to address them. The IRS plans to implement audit logging and review administrator activity on TIC devices. The IRS also plans to fully implement TIC requirements related to Data Loss Prevention, obtain security clearances for operational employees, and complete implementation of proper locations for handling classified information at TIC locations. In addition, the IRS plans to implement vulnerability scanning on TIC equipment and update all TIC equipment to the most current operating systems.

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/201320107fr.pdf>