



Treasury Inspector General for Tax Administration Office of Audit

THE COMPUTER SECURITY INCIDENT RESPONSE CENTER IS EFFECTIVELY PERFORMING MOST OF ITS RESPONSIBILITIES, BUT FURTHER IMPROVEMENTS ARE NEEDED

Issued on March 12, 2012

Highlights

Highlights of Report Number: 2012-20-019 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Computer Security Incident Response Center (CSIRC) is responsible for monitoring the IRS network 24 hours a day year-round for cyberattacks and computer vulnerabilities and for responding to various computer security incidents such as the theft of a laptop computer. Taxpayers are impacted when IRS network disruptions prevent the IRS from performing vital taxpayer services such as processing tax returns, issuing refunds, and answering taxpayer inquiries.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to evaluate the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. TIGTA included this audit in its Fiscal Year 2011 Annual Audit Plan to help fulfill its statutory requirement to review the adequacy and security of IRS technology. This review addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The CSIRC is effectively performing most of its responsibilities for preventing, detecting, and responding to computer security incidents. However, further improvements could be made. The CSIRC's host-based intrusion detection system is not monitoring 34 percent of IRS servers, which puts the IRS network and data at risk. In addition, the CSIRC is not reporting all computer security incidents to the Department of the Treasury, as required. Finally, incident response policies, plans, and procedures are either nonexistent or are inaccurate and incomplete.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Assistant Chief Information Officer, Cybersecurity, direct the CSIRC to 1) develop its Cybersecurity Data Warehouse capability to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system; 2) revise and expand the Memorandum of Understanding with the TIGTA Office of Investigations to ensure all reportable and relevant security incidents are shared with the CSIRC; 3) collaborate with the TIGTA Office of Investigations to create common identifiers to help the CSIRC reconcile its incident tracking system with the TIGTA Office of Investigations' incident system; 4) develop a standalone incident response policy or update the policy in the IRS's Internal Revenue Manual with current and complete information; 5) develop an incident response plan; and 6) develop, update, and formalize all critical standard operating procedures.

The IRS agreed with the recommendations and corrective actions are planned or in process for five of the six recommendations. Although the IRS agreed with the recommendation to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system, its proposed corrective actions did not address the recommendation. Specifically, the IRS did not commit to implementing the controls we recommended.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2012reports/201220019fr.pdf>