Treasury Inspector General for Tax Administration
Office of Audit

UNAUTHORIZED AND INSECURE INTERNAL WEB SERVERS ARE CONNECTED TO THE INTERNAL REVENUE SERVICE NETWORK

Issued on August 26, 2008

Highlights

Highlights of Report Number: 2008-20-159 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

A web server is a computer that contains the software necessary for a web site to operate. At the time of our review, 1,811 internal web servers on the Internal Revenue Service (IRS) network had not been approved to connect to the network, and 2,093 internal web servers connected to the network had at least 1 high-, 1 medium-, or 1 low-risk security vulnerability. These unauthorized and insecure web servers placed both the computers and the entire IRS network at risk of unauthorized access to taxpayer and personally identifiable information.

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 technology. The overall objective was to determine whether the IRS was adequately securing and controlling its web servers.

WHAT TIGTA FOUND

TIGTA identified 1,811 web servers that were not in the web registration database and were not authorized to connect to the IRS network. TIGTA recognizes that some of these unauthorized web servers could be legitimate and support IRS operations. However, the risk exists that the web servers are being used for non-business purposes. Due to time constraints, only limited tests were conducted to identify non-business web servers and none were found. Some unauthorized web servers unintentionally running web services were found.

TIGTA attributed the existence of unauthorized web servers to 1) web server owners not registering their servers with the web registration program, and 2) responsibility for the web registration program remaining unassigned since September 2006. Because no office had responsibility for the web registration program, web servers were allowed to be connected without proper authorization and accountability.

TIGTA also found 2,093 authorized and unauthorized web servers with at least 1 high-, 1 medium-, or 1 low-risk security vulnerability. Unauthorized servers pose a greater risk because the IRS has no way to ensure that they will be continually configured in accordance with security standards when new vulnerabilities are identified. Malicious hackers or disgruntled employees could exploit the vulnerabilities on these web servers to manipulate data on the server or use the servers as launch points to attack other computers connected to the network.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer establish official ownership of and responsibility for the web registration program, enforce IRS procedures to block unauthorized web servers from providing data over the IRS network, and require an annual scan of web servers and comparison to the web registration database to identify unauthorized web servers. Unauthorized web servers should be immediately disconnected from the IRS network, and inappropriate web sites should be referred to the TIGTA Office of Investigations. In addition, the Chief Information Officer should require quarterly network scans of web servers to measure compliance with security requirements.

In their response to the report, IRS officials agreed with our findings and recommendations. The Associate Chief Information Officer, Enterprise Operations, was designated as the responsible official for the web registration program. The IRS plans to identify unauthorized web servers and create a policy and procedure to prohibit them from providing data over the IRS network, and the Computer Security Incident Response Center plans to perform recurring discoveries of enterprise assets and provide an annual report to the web registration business owner to reconcile discovered assets with those currently registered. The IRS plans to disconnect unauthorized web servers and to refer web sites with inappropriate content to the TIGTA Office of Investigations. The Computer Security Incident Response Center plans to perform quarterly security assessment scans to measure compliance with security requirements, and the IRS plans to hold business owners and system administrators responsible for eliminating the vulnerabilities.

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/200820159fr.pdf.

Email Address: inquiries@tigta.treas.gov

Phone Number: 202-622-6500

Web Site: http://www.tigta.gov