



## Treasury Inspector General for Tax Administration Office of Audit

### SECURITY CONTROLS OVER WIRELESS TECHNOLOGY WERE GENERALLY IN PLACE; HOWEVER, FURTHER ACTIONS CAN IMPROVE SECURITY

Issued on September 26, 2011

## Highlights

Highlights of Report Number: 2011-20-101 to the Internal Revenue Service Chief Technology Officer.

### IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) currently uses limited wireless technology but is in the process of expanding its use to help carry out its mission. TIGTA found that controls over wireless technology were generally in place; however, further actions can improve security. Strong security over wireless technology is critical for protecting IRS and taxpayer data from attacker exploits.

### WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Security. The overall objectives of this review were to determine whether the IRS has implemented effective controls to detect unauthorized use of the wireless local area network (WLAN) technology, and to determine whether the IRS's current approved wireless network at its National Distribution Center and its plans for increasing authorized use of WLAN technology at IRS facilities are in accordance with Federal wireless security standards.

### WHAT TIGTA FOUND

While IRS controls over wireless technology were generally in place and operating effectively, TIGTA found areas where improvements can be made. Specifically, IRS network scan data revealed that four users installed and used personal unauthorized wireless devices on their laptops to connect to the IRS network. Although the users of these laptops were authorized to access the network, the use of personal wireless devices is prohibited.

In addition, the IRS developed software to enable laptops to wirelessly connect to the IRS network from non-IRS facilities (home, airport, or hotel) and allowed its use by approximately 300 users before the software was properly tested and approved for use enterprise-wide.

Due to a lack of proper controls, the software was improperly shared and is currently in use on an unknown number of IRS computers, even though the IRS has subsequently abandoned this software and is currently testing a new wireless remote configuration.

In addition, the IRS did not ensure timely monitoring of the wireless router configuration files on the existing approved WLAN.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer 1) implement automated nationwide network scans for unauthorized wireless activity, devices, and software using automated tools and improve incident handling and investigation processes so that when unauthorized wireless activity is identified, subsequent investigations and disciplinary actions are effective; 2) ensure that a security assessment and authorization is completed for all wireless technologies prior to use in the IRS environment, in compliance with IRS policy; and 3) ensure the Enterprise Networks organization takes appropriate action to reinstate monitoring and tracking of configuration files on the WLAN at the National Distribution Center at appropriate intervals to ensure all files are set in accordance with IRS security policy.

The IRS agreed to take corrective actions to address Recommendations 1 and 3, but disagreed with Recommendation 2. The IRS disagreed that IRS policy requires completion of a security assessment and authorization on wireless technologies that it is piloting or demonstrating. TIGTA maintains that prior to placing wireless technologies on the live IRS network, the IRS should ensure that it has completed the required security assessment and authorization.

### READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2011reports/201120101fr.pdf>.

Email Address: [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

Phone Number: 202-622-6500

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