



*Security Controls Over Wireless Technology
Were Generally in Place; However, Further
Actions Can Improve Security*

September 26, 2011

Reference Number: 2011-20-101

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-622-6500

Email Address | TIGTACommunications@tigta.treas.gov

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



HIGHLIGHTS

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

Highlights

**Final Report issued on
September 26, 2011**

Highlights of Reference 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 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.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 26, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: *Michael R. Phillips*
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Controls Over Wireless Technology
Were Generally in Place; However, Further Actions Can Improve
Security (Audit #201120009)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has implemented effective controls to detect the 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. This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Security.

Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Table of Contents

Background	Page 1
Results of Review	Page 4
Controls Over Wireless Technology Were Generally in Place and Operating Effectively	Page 4
Additional Actions Are Needed to Further Improve Security Over Wireless Technology	Page 5
<u>Recommendations 1 and 2:</u>	Page 12
<u>Recommendation 3:</u>	Page 13
Appendices	
Appendix I – Detailed Objectives, Scope, and Methodology.....	Page 14
Appendix II – Major Contributors to This Report	Page 16
Appendix III – Report Distribution List	Page 17
Appendix IV - Management’s Response to the Draft Report.....	Page 18



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Abbreviations

ACIO	Associate Chief Information Officer
ERAP	Enterprise Remote Access Project
EUES	End User Equipment and Services
IRS	Internal Revenue Service
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Background

Wireless technology enables devices to communicate without physical connections, that is, without requiring network or peripheral cabling. It can offer many benefits, such as increased mobility, less costly installation, and easier scalability than wired technologies. However, it can also pose significant risks to the critical infrastructure and assets of an organization if not properly implemented and secured. Wireless communications are vulnerable to interception, denial of service,¹ and deception. The portability and wireless capability of laptops also create considerable risk. The following are examples of well-known attacks used to exploit vulnerabilities in wireless technologies.

Wireless technology can pose significant risks to the critical infrastructure and assets of an organization if not properly implemented and secured.

- *Readily available software tools to intercept and decipher data if strong encryption is not used.* Intercepted wireless traffic may contain sensitive data, such as taxpayer data, or information that can be used to gain unauthorized access to other systems, such as usernames and passwords.
- *Deployment of unauthorized wireless devices, such as access points, that are configured to appear as part of the agency's wireless network infrastructure.* If wireless devices are not adequately secured, they could provide outsiders with an avenue into the internal network and unauthorized access to corporate assets.
- *Eavesdropping on a dual connection that can occur when a laptop is not configured to prevent more than one active Internet connection at a time*—for example, a computer connected to a wired and a wireless network simultaneously can inadvertently become a bridge between a trusted and an untrusted network. Attackers use this bridge to eavesdrop on the user's network communications and potentially gain unauthorized access to the agency's core network.

The Internal Revenue Service (IRS) currently deploys the following types of wireless technology and is in the process of testing and evaluating ways to expand its use as a commitment to improve daily operations for its employees:

- *Wireless local area network (WLAN)*—a group of wireless networking nodes within a limited geographic area that serve as an extension to existing wired local area networks. Wireless networks are also known as Wi-Fi.

¹ A denial of service attack inundates a computer system or network with traffic that overloads the system resources, causing them to cease operations or lose network connectivity.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

- *Wireless remote access software*—this software is used to enable wireless cards on laptops to allow connectivity to a personal or public wireless access point (at home, hotels, or airports) for accessing the Enterprise Remote Access Project (ERAP), which establishes a virtual private network (VPN) for authorized users to access the IRS network.
- *Wireless cellular networks*—a telecommunications network managed by a service provider that supports smartphones, such as the BlackBerry,² which offer the ability to provide data such as email and Internet browsing wirelessly over cellular networks, and cellular data cards, which provide Internet connectivity to laptop computers by accessing cellular networks just as cell phones do.³

The Treasury Inspector General for Tax Administration has conducted two prior audits to detect unauthorized wireless access points at the IRS.

1. Our first audit report on wireless technology was issued in February 2003.⁴ During the audit, we scanned for wireless access points at IRS facilities and found an unauthorized wireless application in one location that was directly connected to the IRS-wide internal network containing sensitive taxpayer information. We also had strong indications of an unauthorized wireless application at another location, although we were unable to locate a wireless device.
2. Our second audit report on wireless technology was issued in March 2007.⁵ During the audit, we reported an unauthorized wireless application in one location was directly connected to the IRS-wide internal network containing sensitive taxpayer information. We also had strong indications of three other unauthorized wireless applications at other locations.

We also reviewed the IRS's one authorized WLAN at the National Distribution Center in Bloomington, Illinois, where wireless devices are used to scan bar codes on IRS publications and forms and to transmit inventory data to a tracking system. During our audit, the IRS Computer Security Incident Response Center,⁶ a part of the Modernization and Information Technology Services organization, conducted penetration tests of the network's wireless infrastructure in January and February 2006 to ensure it was securely configured. The tests identified that one wireless access point was using a default

² BlackBerry phones are locked down and are unable to access the IRS network.

³ Cellular data cards require that users go through the ERAP in order to access the IRS network.

⁴ *Use of Unapproved Wireless Technology Puts Sensitive Data at Risk* (Reference Number 2003-20-056, dated February 21, 2003).

⁵ *Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology* (Reference Number 2007-20-060, dated March 28, 2007).

⁶ Designed to ensure the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computers and data.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

configuration, security devices were not in place to detect attacks against the wireless network, and security configurations were not being monitored. The IRS took immediate action to correct the default configuration and installed a network intrusion prevention system for the wireless network. However, by the end of our audit, the IRS had still not installed the software required to continuously monitor the configuration files of the wireless devices due to other higher priorities. Therefore, we recommended that the IRS take appropriate action to monitor and track the configuration files on the wireless network to ensure all files are set in accordance with current policy.

This review was performed at the New Carrollton Federal Building in New Carrollton, Maryland, in the Office of Cybersecurity during the period January through May 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Results of Review

Controls Over Wireless Technology Were Generally in Place and Operating Effectively

We evaluated the controls the IRS implemented for securing its wireless networks and devices and found that the IRS:

- Established a wireless security policy that was generally in compliance with Federal standards.
- Deployed continuous monitoring procedures for detecting rogue wireless access points and other computing devices using a risk-based approach.
- Uses a VPN to facilitate the secure transfer of sensitive data during remote access using wireless technology.

The IRS still operates its one authorized WLAN at the National Distribution Center, where wireless devices are used to scan bar codes on IRS publications and transmit inventory data to a tracking system. We found that the wireless network components were properly configured, data transmissions were adequately encrypted, and the WLAN generally complied with Federal wireless security standards.

To protect against unauthorized WLANs being deployed elsewhere, the IRS periodically scans its 3 computing centers⁷ and 10 campuses⁸ (and surrounding IRS facilities) using a manual scanning tool. The IRS has never found any unauthorized wireless connections to its network during these scans. Due to resource constraints, the IRS cannot scan all of its offices (approximately 550 facilities). Therefore, it is investigating the procurement of portable scanning devices for use nationwide. In addition, the IRS has initiated implementation of an enterprise asset discovery tool which has the ability to identify unauthorized wireless devices on the network.

As part of IRS Commissioner Schulman's Workforce of Tomorrow strategy, which is to make the IRS one of the best places to work through technology improvements, the IRS is currently evaluating the expansion of two types of wireless technology: deployment of additional WLANs

⁷ IRS computing centers support tax processing and information management through a data processing and telecommunications infrastructure.

⁸ IRS service center campuses are the data processing arms of the IRS. They process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

at IRS facilities and software configurations that allow laptop users to make wireless remote access connections to the IRS network from non-IRS facilities (e.g., hotels, airports, or homes).

With the intent to expand the use of WLANs, the IRS has recently set up test WLANs in two locations as demonstrations that provide wireless access to the IRS network to selected employees. Wireless access points connected to the IRS network allow employees direct access to the network using the built-in wireless network interface cards on their laptops. The IRS completed a risk assessment of this testing process and identified several recommendations for mitigating identified risks.

We confirmed that the IRS took steps to mitigate the risk of dual connection by utilizing a software solution to prevent users from connecting simultaneously to a wireless and wired network and creating an insecure bridge that attackers could exploit. We conducted limited testing of this control and determined that it was in place and operating effectively. We also confirmed that the IRS had changed the name of the wireless access point used in their testing to attract less attention from unauthorized users. Finally, we confirmed that the IRS used the most current authentication and encryption technology available for wireless networks, called Wi-Fi Protected Access, as required by Federal standards.

The IRS is also evaluating the use of wireless remote software configurations that allow laptop users to make wireless remote access connections to the IRS network from non-IRS facilities (e.g., hotels, airports, or homes). In April 2010, the IRS updated its security policy to allow enabling of wireless configurations on laptops to allow users to connect to IRS networks via their built-in wireless network cards and utilizing the ERAP, the agency's secure VPN-based remote access solution. The IRS wrote a software program in Fiscal Year 2010 to start testing the enablement of the built-in wireless network cards, and it is currently working towards an enterprise-wide solution for the usage of this wireless remote access feature.

Additional Actions Are Needed to Further Improve Security Over Wireless Technology

While we found that the IRS was generally complying with Federal wireless security practices, we found four areas where improvements could be made to security over wireless technology used in the IRS.

- Use of automated monitoring to improve detection of unauthorized wireless devices.
- Adherence to IRS policy when developing new wireless technologies.
- Timely monitoring of wireless router configuration files on the existing WLAN.
- Addressing dual connection in IRS policy.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Automated monitoring can better detect unauthorized wireless devices used to access the ERAP

Due to the complexity of properly configuring and ensuring a secure wireless connection, IRS policy requires wireless devices to be acquired and provided by the Modernization and Information Technology Services organization. Additionally, only authorized wireless technologies and devices that have a completed security assessment and authorization by the Modernization and Information Technology Services organization and the Cybersecurity organization, a part of the Modernization and Information Technology Services organization, can be used within the IRS. The purpose of this policy is to ensure that wireless devices are properly configured to comply with the IRS's security policies. IRS policy also prohibits users with administrator privileges from altering any security component configurations or settings on their laptops or desktops without written approval of the Designated Accrediting Authority. In addition, IRS policy prohibits personally owned equipment, such as wireless Universal Serial Bus (USB) devices⁹ as pictured below, from being connected either directly or via VPN to the IRS network.

The Department of the Treasury security policy requires bureaus to ensure that unapproved wireless networking capabilities of laptops and other devices are monitored through automated means for unauthorized changes.

We identified four IRS laptops which used personally owned USB wireless adapters to connect to the IRS network via the ERAP during the time period January to March 2011. USB wireless adapters are not approved for use at the IRS. Administrator privileges were required to install the USB wireless adapter drivers to enable the wireless connection to the ERAP using the USB wireless adapter.



Two of these laptops belonged to IRS employees, and two belonged to contractors. We found three adapters installed on one contractor's laptop. The contractor stated that he tried but was unable to connect to the network with these devices. However, our research revealed that in fact his computer did wirelessly connect to the network with one of these devices.

Each of these users, after making the wireless remote connection, logged onto the IRS network via the ERAP, which requires 2-factor authentication before granting the user access to the IRS network. Although the USB wireless adapters were not authorized, the users were authorized to access the IRS network. However, the installation and use of unauthorized wireless devices is

⁹ Wireless USB adapters allow devices to connect to a wireless network. As of Calendar Year 2010, most newer laptops come equipped with internal adapters, also called wireless network interface cards.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

prohibited by IRS policy because their use could put the IRS at risk of unauthorized access to its network and data. We did not evaluate the security configurations of these laptops. However, during the installation, users with administrative privileges could inadvertently or intentionally alter security settings that could expose the laptops to attacker exploits. For example, if the users do not ensure that configurations are set to prevent dual connections, attackers could gain unauthorized access to the IRS network.

We identified these four laptops using a snapshot of IRS network scan data from Tivoli,¹⁰ collected once a week over a 6-week period, and device data collected by the IRS asset discovery tool called Business DNA.¹¹ The IRS's current wireless monitoring efforts using their manual scanning tool would not have identified these instances of personal USB wireless adapters because the scanning at the computing centers and campuses is looking for wireless access points. Enhancing the IRS's current manual scanning at its main sites with the use of the IRS's already available automated scanning tools that collect data enterprise-wide can improve its continuous monitoring and detection of rogue wireless software and devices. This method would lower the resources needed while achieving enterprise-wide scanning coverage and provide data on both unauthorized wireless access points and the use of unapproved wireless software and devices.

In addition, we provided the IRS Computer Security Incident Response Center and the End User Equipment and Services (EUES) organization, divisions within the Modernization and Information Technology Services organization, with the documentation for the four laptops that used the wireless USB adapters (including the specific laptops and names of the laptop owners). However, in response to the noncompliant activity we identified, the IRS was unable to complete sufficient follow-up activities to ensure the illegal wireless software was removed and disciplinary actions were taken as necessary. Without adequate processes to handle incidents of noncompliance with IRS security policy, the noncompliant activity may continue to put the IRS network at risk of attacker exploits.

Adherence to policy when developing new wireless technologies needs improvement

IRS policy requires that all wireless remote configurations must go through the Enterprise Life Cycle¹² process and be approved by the Associate Chief Information Officer (ACIO),

¹⁰ The Tivoli® applications provide the IRS with the ability to systemically deliver the most current versions of software and updated security patches to employees' computers and to scan the network for maintaining computer inventory records.

¹¹ Business DNA is an asset discovery tool that provides detailed hardware and software configuration information for all devices connected to the network. The Department of the Treasury recently selected Business DNA as the enterprise tool for all bureaus to use in information technology asset discovery, inventory, and reporting.

¹² A structured business systems development method that requires the preparation of specific work products during different phases of the development process.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Cybersecurity. In addition, all wireless networks and devices must have a completed security assessment and authorization before they are used within the IRS.

Further, the National Institute of Standards and Technology¹³ recommends that agencies establish and enforce usage restrictions and implementation guidance for wireless access. According to the National Institute of Standards and Technology standards, security policies should identify which users are authorized to connect wirelessly to an agency's networks, detail which wireless-enabled devices can connect to the agency's networks remotely, and describe the types of external networks permitted. For example, policies should specify if users connecting remotely through public hot spots to an agency's networks are authorized to use only agency-issued mobile devices. In addition, the Department of the Treasury security policy requires bureaus to establish usage restrictions and implementation guidance for wireless technologies and to document, monitor, and control wireless access to the information system.

As previously mentioned, the IRS is evaluating the expansion of two types of wireless technology for its employees.

Expansion of the WLAN at IRS Facilities. Contrary to its wireless security policy, the IRS did not intend to conduct a security assessment and authorization until after its WLAN demonstrations on the IRS network were complete. The IRS planned to take what they learned from these demonstrations, make final decisions on equipment needs, and then proceed with the formal security assessment and authorization process. The IRS also stated that conducting the demonstration on the production network would give them a better sense of what the true implications of the WLAN would be and would allow a large number of people to participate.

However, after we began our review, the Cybersecurity organization completed a risk assessment of the WLAN security controls in February 2011, and the Designated Accrediting Authority signed a memorandum accepting the reported risks and authorizing the demonstrations to operate on the IRS production network. In addition, the Architecture and Implementation division, a part of the Cybersecurity organization, signed a waiver for the WLAN's use of products not yet approved for use in the IRS environment. We reviewed the components of the WLAN being demonstrated at the New Carrollton Federal Building and found the WLAN generally complied with Federal security requirements for wireless networks.

Expansion of Wireless Remote Access by Employees. The wireless remote configuration in use at the IRS to access the ERAP had not been properly assessed or approved for use in the IRS environment. In early 2010, a wireless configuration was developed to provide IRS employees wireless access to the IRS network while at off-site locations such as hotels and airports. According to EUES organization management, approximately 300 users were allowed to

¹³ The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

participate in a limited demonstration of the technology at an IRS conference in May 2010. Rather than removing the wireless capability from the users until proper security testing and approvals of the configuration were completed, EUES organization officials informed us that the configuration remains in use. They also informed us that controls were not in place to prevent the configuration from being shared with unauthorized users, and that they believed the configuration was in fact being shared with users that were not a part of the May 2010 demonstration. We identified 12 users who were not associated with the May 2010 demonstration but used a wireless remote configuration to access the ERAP during January through March 2011.

The ACIO, Cybersecurity, disagreed that this software that was demonstrated in May 2010 required the completion of the Enterprise Life Cycle or a security assessment and authorization at this stage in its development. The ACIO stated that the EUES and Cybersecurity organizations planned to evaluate how wireless remote access worked in the production environment and gather feedback from the users at the demonstration to help shape the ultimate design of the wireless solution for when it is deployed. In addition, the ACIOs of the Cybersecurity and EUES organizations indicated they were not concerned about, and had no need to know, which users and computers have the unapproved configuration installed, as use of the configuration poses no security risk because the ERAP process controls access to the IRS network.

We did not identify any security vulnerabilities related to this configuration. However, as system administrators install this configuration for themselves or for others, we believe that settings could be changed that leave vulnerabilities exposed. We also believe that the IRS should know which users and computers have installed software while still in a demonstration phase, in the event that the IRS determines the configuration did not meet current or future IRS standards or requires security patches or updates until an enterprise-wide solution is approved.

The IRS shared with us that this software had subsequently been abandoned for a new wireless remote configuration, which is currently undergoing testing. The IRS has no idea on which laptop computers the older configuration resides. As a result, unapproved and untested software is currently in use on an unknown number of IRS computers. If security problems are discovered during testing of the new configuration that may also affect the old one, the IRS cannot ensure the removal of the old configuration.

IRS policy helps to ensure proper controls are placed over the development and use of wireless remote configurations. Without adhering to these controls, the IRS risks the introduction of configurations into the production environment that could contain security vulnerabilities.

For both wireless expansion efforts, the ACIO, Cybersecurity, and Treasury Inspector General for Tax Administration disagreed on how to interpret IRS policy, which states that wireless networks, devices, and remote access configurations must have a completed security assessment and authorization before they are used within the IRS. The ACIO, Cybersecurity, believed IRS



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

use of the WLAN networks and wireless remote configuration software prior to completion of a security assessment and authorization was not contrary to IRS policy because (1) wireless access to the IRS network is no longer prohibited (based on the April 2010 policy update); (2) the demonstration-type testing of wireless technologies is intentionally performed prior to beginning the Enterprise Life Cycle to allow the IRS to determine what wireless components it plans to implement enterprise-wide and, once determined, would then warrant completion of the Enterprise Life Cycle milestone, testing, and approval processes; and (3) he was aware and had verbally approved of the actions taken in both the WLAN and wireless remote configuration instances.

We are concerned that, without requiring proper security assessments and authorizations before allowing use of wireless technology in the IRS environment, security flaws could exist in the untested technology that could leave the IRS open to attacks that exploit wireless networks or transmissions.

Corrective action to ensure timely monitoring of configuration files, taken in response to a prior audit finding at the National Distribution Center, was not effective

To minimize network security vulnerabilities and exposures, the IRS guidelines, standards, and procedures require IRS staff to periodically assess compliance of all network components, such as switches and routers. IRS staff should use configuration validation tools to measure compliance against the established security baseline.

The IRS currently has one authorized WLAN at its National Distribution Center, where wireless devices are used to scan bar codes on IRS publications and transmit inventory data to a tracking system. In March 2007, we reported that the IRS was not adequately monitoring the security configurations on the WLAN. The IRS agreed to monitor the configuration files on the WLAN on a monthly basis to ensure all configurations adhered to IRS standards.

During our current review, we found that the IRS had not been conducting the manual monthly reviews of the configuration files for the two switches on the WLAN as they had agreed to do in response to our prior finding. Per the IRS, the last validation of the configuration files for these switches occurred during December 2009.

The cause for not monitoring configurations as planned was due to a reorganization of the territory and loss of personnel. Enterprise Network organization managers, a part of the Modernization and Information Technology Services organization, failed to identify and reassign this responsibility after the employee who had been responsible for the monthly manual monitoring had been transferred. Enterprise Network organization managers assumed the configuration files for these switches were being captured electronically and reviewed remotely.

The Enterprise Network organization staff informed us that the configuration files for these two switches cannot be reviewed remotely because these switches sit behind the devices that encrypt



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

the wireless network. The Enterprise Network organization staff also informed us that they believe manually pulling the configurations for these switches every 3 months, rather than monthly, would be adequate. They believe the less frequent reviews would be adequate due to the wireless detection systems they have installed, the infrequent changes to the switches, and the cost of manpower and travel to the site to conduct the reviews.

Network switches provide services that are essential to the operation of the IRS local area networks and the customers they serve. Poor security can expose the entire IRS network, components, and configurations to attackers whose goal is to reduce network and data integrity. Compromise of a network switch can lead to reduced performance, denial of service, and exposure of sensitive taxpayer data. Inadequate monitoring of the configuration files for the wireless network switches could increase the likelihood of the network being compromised and operations disrupted.

Security policy did not address dual connection

The National Institute of Standards and Technology guidelines recommend that laptops be configured to not allow the simultaneous use of more than one network interface; that is, the wireless capability of the laptop should be turned off or disabled when the laptop is connected to the agency's wired network. If wireless-enabled laptops are not configured to prevent simultaneous (or dual) connections, an attacker could connect to the laptop's wireless interface while the laptop is connected to the agency's wired network, potentially allowing the attacker unauthorized access to the agency network.

The Government Accountability Office reported in November 2010 that many agencies had not addressed the risk of dual connection of laptops in their security policies, and none of the five agencies where the Government Accountability Office conducted detailed testing had implemented controls to prevent it.

We reviewed the IRS's wireless security policy and found that it did not address the risk of dual connection on wireless-enabled laptops. We also noted that the Department of the Treasury security policy did not address dual connection in November 2010; however, it issued a security policy update in March 2011 that does address dual connection.

The IRS informed us that the software installed on users' laptops to enable WLAN connectivity for participating in the demonstrations includes an "exclusive connection" feature which allows no more than one active connection at a time and therefore addresses the dual connection risk. We tested this control during our visit to New Carrollton and found that it worked effectively to prevent dual connection.

However, until the IRS fully documents policies prohibiting dual connections, an increased risk exists that future wireless technology projects may not implement sufficient controls to address this risk, potentially allowing an attacker to exploit this vulnerability and gain unauthorized access into the IRS network to destroy, modify, or copy sensitive information.



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Management Action: The IRS updated the Internal Revenue Manual during our fieldwork to address the condition above. The Internal Revenue Manual now requires that WLAN clients be configured so only one active physical network connection is possible, either wired or wireless, at any time and that WLAN clients be configured to prevent dual connections.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Implement automated nationwide network scans for unauthorized wireless activity, devices, and software using Tivoli or Business DNA, and improve processes to handle incidents of noncompliance with IRS security policy so that when unauthorized wireless activity is identified, subsequent investigations and disciplinary actions are effective.

Management's Response: The IRS agreed with this recommendation. The IRS will use a set of automated tools to determine wireless activity, devices, and software as part of full deployment of a wireless strategy. In conjunction with the automated tools, the IRS will incorporate the use of wireless network scanners in areas where it determines there is the potential for the greatest risk.

Recommendation 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.

Management's Response: The IRS disagreed with this recommendation. IRS policy does not require completion of a security assessment and authorization on technologies, but rather on information systems. IRS policy requires that new technology, such as wireless technology, undergo security assessment and authorization when it is utilized by an IRS information system that is being designed, developed, and expected to be ultimately deployed into full production. In the case of the wireless pilot, a risk assessment was performed and the Authorizing Official authorized the pilot to begin. However, a full security assessment and authorization for the wireless pilot would be premature as the wireless pilot was still in the design phase and being conducted in an area where users had little access to taxpayer data. Performing security assessment and authorizations on pilots, tests, and/or demonstrations would not allow the IRS the ability to make effective risk-based decisions regarding the appropriate, secure, and cost-effective use of what in this case was wireless technology.

Office of Audit Comment: We agree that IRS policy would not require the completion of a security assessment and authorization if the IRS conducted its wireless pilots and demonstrations on a test network. However, the IRS placed the wireless pilot on the live IRS network. Likewise, the IRS demonstrated the wireless remote access configuration that still provides an unknown number of users access to the live IRS network prior to completing any security assessment and authorization activities. At the



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

start of our review, the IRS had informed us that it did not plan to perform any security assessment and authorization activities for its wireless pilots or demonstrations. We agree that the risk assessment that the IRS subsequently conducted prior to deploying the wireless pilot helped to mitigate potential risks. However, prior to piloting, demonstrating, or any use of wireless technology on the live IRS network, we continue to recommend that the IRS remain diligent in completing commensurate security assessment and authorization activities in compliance with IRS policy in order to detect and avoid security risks that could leave the IRS open to attacks.

Recommendation 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.

Management's Response: The IRS agreed with this recommendation. Enterprise Networks has assigned the site to an employee to reinstate routine monitoring and tracking of configuration files on the WLAN at quarterly intervals to ensure all files are set in accordance with IRS security policy.



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Appendix I

Detailed Objectives, Scope, and Methodology

Our objectives were to determine whether the IRS has implemented effective controls to detect the unauthorized use of the WLAN technology, and to determine whether the IRS's current approved WLAN at its National Distribution Center and its plans for increasing the authorized use of WLAN technology at IRS facilities are in accordance with Federal wireless security standards. To accomplish these objectives, we:

- I. Evaluated the adequacy of IRS policies related to wireless technology.
- II. Evaluated IRS efforts at identifying unauthorized wireless access points and devices.
 - A. Determined whether IRS corrective action from our prior report¹ was implemented.
 - B. Obtained and reviewed Tivoli² and Business DNA³ data.
- III. Provided information to the IRS (for further investigation) on any potential unauthorized devices or access points we identified.
- IV. Identified software utilities that may be able to remotely scan for unauthorized wireless activity.
- V. Determined whether the IRS-approved WLAN at the National Distribution Center was configured in accordance with Federal wireless security standards.
 - A. Determined whether IRS corrective action from our prior report⁴ was implemented.
 - B. Obtained and reviewed the current WLAN design documentation.
- VI. Determined whether the IRS's plans for increasing the authorized use of WLAN technology at IRS facilities was in accordance with Federal wireless security standards.
 - A. Obtained and reviewed the IRS design documents for its WLAN demonstration.

¹ *Use of Unapproved Wireless Technology Puts Sensitive Data at Risk* (Reference Number 2003-20-056, dated February 21, 2003).

² The Tivoli® applications provide the IRS with the ability to systemically deliver the most current versions of software and updated security patches to employees' computers and to scan the network for maintaining computer inventory records.

³ Business DNA is an asset discovery tool that provides detailed hardware and software configuration information for all devices connected to the network. The Department of the Treasury recently selected Business DNA as the enterprise tool for all bureaus to use in information technology asset discovery, inventory, and reporting.

⁴ *Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology* (Reference Number 2007-20-060, dated March 28, 2007).



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

- B. Determined whether the IRS WLAN demonstration design documents met Federal standards for deploying and monitoring a secure WLAN.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: the IRS's policies, procedures, and practices for ensuring wireless technology is compliant with Federal standards. We evaluated these controls by interviewing Cybersecurity and EUES organization officials, reviewing network scan data, evaluating design documentation of the existing and planned WLANs, and testing WLAN demonstration components.



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Larry Reimer, Audit Manager, Technical Audit Group
Cari Fogle, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Victor Taylor, Auditor



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Chief Counsel CC
Director, Wage and Investment Business Systems Planning SE:W:BMO:BSP
Director, Office of Program Evaluation and Risk Analysis RAS:O
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison:
 Director, Risk Management Division OS:CTO:SP:RM



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Appendix IV

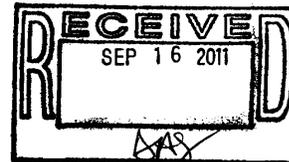
Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

September 9, 2011



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report –Security Controls Over
Wireless Technology Were Generally in Place;
However, Further Actions Can Improve Security
(Audit # 201120009)
(e-trak # 2011-238700)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss your observations. As a result of these meetings, the audit team incorporated some of our suggestions into the draft report.

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. We agree that strong security over wireless technology is critical for protecting IRS and taxpayer data from attacker exploits. We acknowledge that our continued diligence is necessary to ensure taxpayer data are fully protected.

We agree with recommendations one and three and will proceed as noted in our detailed attachment. However, we believe our existing procedures satisfy the requirements for recommendations two and as such, disagree with the recommendation made as part of your report.

We are committed to continuously improving security on our information technology systems and processes. Your continued support and the assistance your team provides have been a valuable resource to our organization. If you have any questions, please contact me at (202) 622-6800 or Andrea Greene-Horace at (202) 283-3427.

Attachment



Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security

Draft Audit Report – Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security – Revised Management Response (Audit # 201120009) (i-trak # 2011-23870)

RECOMMENDATION #1: The Chief Technology Officer should implement nationwide network scans for unauthorized wireless activity, devices, and software using Tivoli or Business DNA, and improve processes to handle incidents of noncompliance with IRS security policy so that when unauthorized wireless activity is identified, subsequent investigations and disciplinary actions are effective.

CORRECTIVE ACTION #1: We agree with the recommendation to use a set of automated tools to determine wireless activity, devices and software as part of full deployment of a wireless strategy. In conjunction with the automated tools we will incorporate the use of wireless network scanners in areas where we determine there is the potential for the greatest risk.

IMPLEMENTATION DATE: September 28, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should 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.

CORRECTIVE ACTION #2: The IRS disagrees with this recommendation. TIGTA suggests that IRS follow existing Service policy, IRS believes it is compliant. Specifically, IRM 10.8.40.3.4(1) states "All wireless networks and devices shall obtain C&A/Security Authorization in accordance with IRM 10.8.1." And, IRM 10.8.1.3.4 "Security Assessment and Authorization (SA&A)," specifically states SA&A shall be conducted on 'IRS information systems'. An information system by definition is a 'discreet set of information resources', IRS believes the IRM supports the IRS position that SA&A's are not conducted on technologies. Rather, per the IRM, any new technology, such as wireless technology, is required to undergo SA&A when it is utilized by an IRS information system that is being designed, developed and is expected to be ultimately deployed into full production.



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

Draft Audit Report – Security Controls Over Wireless Technology Were Generally in Place;
However, Further Actions Can Improve Security – Revised Management Response (Audit #
201120009) (i-trak # 2011-23870)

Where 10.8.40.3.4 (2) states, “Only authorized wireless technologies and devices that
are certified and authorized by MITS and the ACIO Cybersecurity shall be used within
the organization,” it is qualified by 10.8.40.3.4 (1) referenced above.

In the case of IRS’s wireless pilot, a risk assessment was performed to allow the IRS to
understand what risks might exist so that the responsible Authorizing Official could
make an informed decision before he or she signed a memo authorizing the pilot to
begin. Also, a full SA&A for the pilot would be premature as the wireless network was
still in a design phase and being conducted in an area where users had little access to
any taxpayer data.

Additionally, Cybersecurity does not perform SA&A on pilots, tests, and/or
demonstrations, nor does the IRS conduct SA&A on applications or General Support
Systems prior to entering the Enterprise Life Cycle. To do so would be fiscally
irresponsible and would not allow the agency the ability to make effective risk-based
decisions regarding the appropriate, secure, and cost effective use of what in this case
was wireless technology.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #3: The Chief Technology Officer should 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.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. Enterprise
Networks has taken the appropriate action by assigning the site to an employee to
reinstate routine monitoring and tracking of configuration files on the WLAN at the
National Distribution Center at quarterly intervals to ensure all files are set in
accordance with IRS security policy.

IMPLEMENTATION DATE: May 30, 2011 (Completed)

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks



*Security Controls Over Wireless Technology Were Generally
in Place; However, Further Actions Can Improve Security*

- Draft Audit Report – Security Controls Over Wireless Technology Were Generally in Place;
• However, Further Actions Can Improve Security – Revised Management Response (Audit #
201120009) (i-trak # 2011-23870)

CORRECTIVE ACTION MONITORING PLAN: N/A