TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology

March 28, 2007

Reference Number: 2007-20-060

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 | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 28, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology (Audit # 200620029)

This report presents the results of our review of the Internal Revenue Service's (IRS) wireless security policy and program. The overall objective of this follow-up review was to determine whether IRS assets are at risk from the use of unapproved wireless network devices. We also evaluated the security controls over the one IRS-approved wireless network. In addition, we determined whether existing wireless networks were properly approved and securely implemented and whether IRS employees or contractors were installing unapproved wireless networks. This audit was part of the statutory audit coverage under the Information Systems Programs and is included in the Treasury Inspector General for Tax Administration Fiscal Year 2006 Annual Audit Plan.

Impact on the Taxpayer

The use of wireless technology is growing at a phenomenal rate because of its convenience, affordability, and mobility; however, the use of wireless technology also poses significant security risks. We identified an unauthorized wireless device in one location and had strong indications of three other wireless devices at other locations. If unauthorized wireless devices are installed and connected to the IRS network, sensitive financial data for over 226 million taxpayers could be at risk.

Synopsis

Wireless technology is based on sending radio-wave transmissions through the air between two points, usually a user laptop computer and a predefined access point that can be connected back

to the organization's network to allow for full functionality and access to all computer resources. Wireless signals can be intercepted by anyone in close proximity with inexpensive, readily available equipment. Although encryption is available for wireless traffic, it has proven to be weak, and free software is widely available on the Internet to break this encryption.

In February 2003, we issued a report[1] that addressed the IRS' actions to control and secure the use of wireless technology. We reported an unauthorized wireless application in one location was directly connected to the IRS-wide internal network containing sensitive taxpayer information, and we had strong indications of another unauthorized wireless application at another location. We recommended the IRS immediately disconnect all unapproved wireless networks, issue policies and procedures for the use of wireless technology, and ensure wireless scanning efforts include sufficient geographic coverage.

To correct the deficiencies we reported, the IRS disconnected the unauthorized wireless network and developed a comprehensive wireless security policy that requires the Mission Assurance and Security Services organization to approve all requests for deploying wireless networks and devices. In addition, the IRS has scanned offices to search for unauthorized wireless devices. Although the IRS took several corrective actions, in this review we identified similar weaknesses that could jeopardize sensitive taxpayer systems and information.

We scanned 20 IRS buildings in 10 cities using inexpensive wireless equipment and software freely available on the Internet. During our scanning efforts, we identified an unauthorized wireless device in one location and had strong indications of three other wireless devices in other locations. The wireless access point we located was not directly connected to the IRS network. However, anyone with a wireless detection tool could pick up the wireless signal and gain access to the computer. Also, if an employee connected to the access point with an IRS computer, and the access point was configured improperly, a hacker conceivably could gain access to the IRS network.

The IRS is currently attempting to detect unauthorized access points on an ad hoc basis, with limited success. As of May 2006, it had scanned fewer than 6 percent of all IRS locations and had concentrated mainly on the Washington, D.C., and Baltimore, Maryland, areas. We believe this scanning is of limited value, considering wireless access points can be set up easily anywhere in the nation and can place the confidentiality of the data at risk.

The IRS has one authorized wireless network; it is located in Bloomington, Illinois. The Enterprise Logistics Information Technology (ELITE) network is used to receive, store, and distribute IRS published products; it is considered by the IRS to be a low security risk. The IRS Computer Security Incident Response Center conducted penetration tests of the ELITE network's wireless infrastructure in January and February 2006 to ensure it was securely

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

configured. The tests identified that one wireless access point was using a default configuration, security devices were not in place to detect attacks against the ELITE 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 ELITE wireless network. However, the Enterprise Networks Division has not installed the software required to continuously monitor the configuration files of the wireless devices due to other higher priorities.

Recommendations

To detect and deter employees from installing unauthorized wireless access points, we recommended the Chief, Mission Assurance and Security Services, use available tools to proactively scan, on a continuous basis, the entire IRS network for unapproved wireless devices and periodically advise employees of the risk involved with wireless technology. The risk and consequences for violating the current wireless policy should also be included in the IRS' annual security awareness training. In addition, the Chief Information Officer should ensure the Enterprise Networks Division takes appropriate action to monitor and track the configuration files on the ELITE wireless network to ensure all files are set in accordance with current policy.

Response

The IRS agreed with all of our recommendations. The Mission Assurance and Security Services organization established a monthly wireless scanning project, initiated monthly scans in November 2006 that included the nine IRS campuses[2] and three IRS Computing Centers, and will expand the number of locations scanned after performing a risk-based evaluation. In addition, the Mission Assurance and Security Services organization will include information about the IRS wireless policy, risks associated with wireless technology, and the consequences for policy violations in the mandatory annual security awareness training. The Enterprise Networks Division is currently working with the Mission Assurance and Security Services organization to fully assess and manage the ELITE network devices to ensure all configurations adhere to IRS standards. Management's complete response to the draft report is included as Appendix V.

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 Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

[2] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
ELITE	Enterprise Logistics Information Technology
IRS	Internal Revenue Service

Background

The use of wireless technology is growing at a phenomenal rate because of its convenience, affordability, and mobility. These benefits that make wireless technology so useful and attractive to its users also pose significant security risks.

Ninety-five percent of corporate laptop computers shipped in 2005 were equipped for wireless operation.

Wireless technology is based on sending radio-wave transmissions through the air between two points, usually a user laptop computer and a predefined access point that can be connected back to the organization's network to allow for full functionality and access to all computer resources. Wireless signals can be intercepted by anyone in close proximity with inexpensive, readily available equipment. Although encryption is available for wireless traffic, it has proven to be weak. Free software is widely available on the Internet to break this encryption.

Loosely organized hacker and investigative groups have been scanning metropolitan areas for wireless technology for some time. Commonly referred to as "war driving," this activity has more recently been extended to hackers posting information on locations of insecure wireless networks for others to potentially exploit.

Sensitive financial data for over 226 million taxpayers' accounts could be at risk if an unapproved wireless device was installed and connected to the IRS network.

The Privacy Rights Clearinghouse[1] reports that personal information of over 100 million Americans has been compromised since February 2005. More than 50 percent of the damage came from intruders who were not authorized to access the information, several of whom used wireless attacks. For the Internal Revenue Service (IRS), the security risks associated with wireless technology mainly involve the improper access to and unauthorized disclosure of sensitive taxpayer data.

In February 2003, we issued a report[2] that addressed the IRS' actions to control and secure the use of wireless technology. We reported an unauthorized wireless application in one location was directly connected to the IRS-wide internal network containing sensitive taxpayer information, and we had strong indications of another unauthorized wireless application at another location, although we were unable to locate a wireless device.

[1] The Privacy Rights Clearinghouse is a nonprofit consumer organization with a two-part mission: consumer information and consumer advocacy.

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

As of January 2007, the IRS had only one approved wireless network, the Enterprise Logistics Information Technology (ELITE) network, which is an integrated, web-based, real-time system used to receive, store, and distribute IRS published products at the National Distribution Center in Bloomington, Illinois. The ELITE network, specifically used for order management, inventory management, and distribution of products, is designated by the IRS as a low security risk.

We performed the review at the offices of the Chief Information Officer and the Chief, Mission Assurance and Security Services, in Washington, D.C., and at IRS offices located in Dallas, Fort Worth, and Houston, Texas; Plantation, Miami, and West Palm Beach, Florida; Denver, Colorado; Portland, Oregon; Atlanta, Georgia; and Bloomington, Illinois, during the period April through November 2006. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objectives, scope and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

In our February 2003 report, we recommended the IRS immediately disconnect all unapproved wireless networks, issue policies and procedures for the use of wireless technology, and ensure wireless scanning efforts include sufficient geographic coverage. To correct the deficiencies we reported, the IRS disconnected the unauthorized wireless network and took several other corrective actions. However, in this review we identified similar weaknesses that could jeopardize sensitive taxpayer systems and information.

Corrective Actions Were Taken; However, We Continue to Locate Unauthorized Wireless Devices

Based on the prior report recommendations, the IRS developed a comprehensive wireless security policy consistent with standards, best practices, and guidance from the Department of the Treasury, the National Institute of Standards and Technology,[3] and the United States Government Accountability Office and issued the policy in March 2006. The policy incorporated guidance from some of the industry security leaders such as the Department of Defense, Defense Information System Agency,[4] and Center for Internet Security.[5] The policy requires that the IRS Mission Assurance and Security Services organization approve all requests for deploying wireless networks and devices. All authorized wireless systems must be certified and accredited by the IRS Modernization and Information Technology Services and the Mission Assurance and Security Services organizations.

To complement the wireless security policy, the IRS Computer Security Incident Response Center (CSIRC)[6] and the Treasury Inspector General for Tax Administration Office of Investigations System Intrusion Network Attack Response Team jointly conduct periodic scans to detect any unauthorized wireless devices at selected IRS facilities. Over the last several years, they have conducted approximately 30 wireless scans mainly in and around Washington, D.C., including the New Carrollton Federal Building and Baltimore, Maryland, field offices. Other locations were scanned based on allegations from either the IRS or Treasury Inspector General

[3] The National Institute of Standards and Technology's mission is to promote United States innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
[4] An agency in the Department of Defense responsible for developing, operating, and supporting information systems to serve the needs of the President, the Secretary of Defense, and the Joint Chiefs of Staff.
[5] A nonprofit enterprise whose mission is to help organizations reduce the risk of business and electronic commerce disruptions resulting from inadequate technical security controls.
[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.

for Tax Administration employees. Through their joint efforts, one unapproved wireless access point connected to the IRS network was detected in an office in Dallas, Texas.

We scanned 20 IRS buildings in 10 cities using inexpensive wireless equipment and software[7] freely available on the Internet. During our scanning efforts, we identified an unauthorized wireless device in one location and had strong indications of three other wireless devices at other locations. Appendix IV includes a complete list of the locations we scanned for wireless devices.

The IRS Criminal Investigation Division in Denver, Colorado, had connected one unauthorized wireless access point to a desktop computer (see Figures 1 and 2). The device was not connected to the IRS' network but had its own Digital Subscriber Line (commonly known as DSL)[8] connected to it. The former Director, Special Investigative Techniques Division, approved the purchase of the device. The Denver Criminal Investigation Division Lead Development Center uses the device to log onto the Internet as an undercover computer to assist with investigations. The device was originally installed with the wireless features turned off by default; so someone within the office configured the device for wireless capabilities. Neither of the two system administrators could explain to us why the wireless features were turned on, only that the device is rarely used. However, on the morning we scanned the office, the wireless device was activated and operating, and when we returned in the afternoon, it had been turned off. The system administrators stated they were aware of the IRS' wireless security policy but did not believe they had violated the policy because the wireless access point was not connected to a computer on the IRS network.

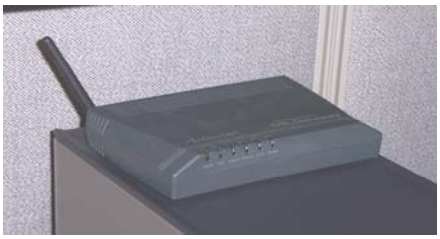

Figure 1: Wireless access point.

Figure 2: Criminal Investigation Division computer with wireless access point.

Although the wireless access point was not directly connected to the IRS network, our concern is that anyone with a wireless detection tool could pick up the wireless signal and gain access to the computer. Also, if an employee connected to the access point with an IRS computer, and the access point was configured improperly, a hacker conceivably could gain access to the IRS network. Once the device was located and identified, the Treasury Inspector General for Tax Administration Office of Investigations was contacted to remove the wireless access point and eliminate the vulnerability.

[7] We used Kismet, a free online tool used to detect the presence of both wireless access points and wireless clients and associate them to each other.

[8] A Digital Subscriber Line provides digital data transmission over the wires of a local telephone network.

In addition, we detected strong wireless signals at three other facilities but were unable to pinpoint where the access points were located. The strength of the signals indicated some kind of wireless activity. We were advised that an unauthorized wireless access point was in use prior to our arrival in at least one location.

We found strong indications of wireless access points at three different IRS locations.

Currently, the IRS is attempting to detect unauthorized access points on an ad hoc basis, with limited success. As of May 2006, it had scanned fewer than 6 percent of all IRS locations and had concentrated mainly on the Washington, D.C., and Baltimore, Maryland, areas. We believe this scanning is of limited value, considering wireless access points can be set up easily anywhere in the nation and can place the confidentiality of the data at risk. In addition, the IRS has not used available tools that continuously monitor network traffic for malicious or accidental wireless activities. These tools can provide additional protection, regardless of the location, and provide immediate detection. We also believe employees were not aware of the risks of establishing wireless access points.

Recommendations

Recommendation 1: The Chief, Mission Assurance and Security Services, should use available tools to proactively scan, on a continuous basis, the entire IRS network for unapproved wireless devices.

> ***Management's Response:*** IRS management agreed with this recommendation. The Mission Assurance and Security Services organization established a monthly wireless scanning project, initiated monthly scans in November 2006 that included the nine IRS campuses[9] and three IRS Computing Centers, and will expand the number of locations scanned after performing a risk-based evaluation.

Recommendation 2: The Chief, Mission Assurance and Security Services, should periodically advise employees of the risk involved with wireless technology. The risk and consequences for violating the current wireless policy should also be included in annual security awareness training.

> ***Management's Response:*** IRS management agreed with this recommendation. The Mission Assurance and Security Services organization will include information about the IRS wireless policy, risks associated with wireless technology, and the consequences for policy violations in the mandatory annual security awareness training.

[9] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

Most Corrective Actions Have Been Taken to Ensure Adequate Security of the Enterprise Logistics Information Technology Wireless Network

The IRS has one authorized wireless network; it is located in Bloomington, Illinois. The ELITE network is an integrated, web-based, real-time supply chain system used to receive, store, and distribute IRS published products. The IRS considers it to be a low security risk. The current IRS wireless policy states all approved wireless networks shall adhere to specific security requirements that include:

- Wireless networks and devices transmitting Sensitive But Unclassified information shall obtain certification and accreditation.
- An intrusion detection system shall monitor the wireless environment and immediate surrounding areas.

The CSIRC conducted penetration tests of the ELITE network's wireless infrastructure in January and February 2006 to ensure it was securely configured, followed the current policy, and was not susceptible to any known attacks. During its reviews, the CSIRC identified the following issues:

- One access point on the wireless network was still using its default configuration. The IRS took immediate corrective action, making the necessary changes to ensure all access points were properly and consistently configured. On March 9, 2006, the IRS certified and accredited the ELITE wireless network and accepted the security risks identified.
- Security devices were not in place to detect attacks against the ELITE wireless network. Subsequently, in May 2006, the CSIRC installed a Network Intrusion Prevention System, which automatically blocks malicious attacks against this wireless network. Potential attacks are continuously monitored by the CSIRC.
- Security configurations were not monitored on the ELITE wireless network. Inadvertent or intentional changes to the security configurations could increase the likelihood that the network could be compromised and operations disrupted. The CSIRC recommended the Enterprise Networks Division within the Modernization and Information Technology Services organization monitor the security configuration settings of the devices on the wireless network. At the time of our review, the Enterprise Networks Division had not installed the software required to continuously monitor the configuration files of the wireless devices, as recommended, due to other higher priorities.

Recommendation

Recommendation 3: The Chief Information Officer should ensure the Enterprise Networks Division takes appropriate action to monitor and track the configuration files on the ELITE wireless network to ensure all files are set in accordance with the IRS wireless security policy.

> ***Management's Response:*** IRS management agreed with this recommendation. The Enterprise Networks Division is currently working with the Mission Assurance and Security Services organization to fully assess and manage the ELITE network devices to ensure all configurations adhere to IRS guidelines, standards, and procedures.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objective for this follow-up review was to determine whether IRS assets are at risk from the use of unapproved wireless network devices. We also evaluated the security controls over the one IRS-approved wireless network. In addition, we determined whether existing wireless networks were properly approved and securely implemented and whether IRS employees or contractors were installing unapproved wireless networks. To accomplish our objective, we:

I. Determined whether the IRS had developed and implemented policies, procedures, and guidance for the use of wireless technology.

   A. Determined what corrective actions were taken on the recommendations from our prior audit report entitled, *Use of Unapproved Wireless Technology Puts Sensitive Data at Risk* (Reference Number 2003-20-056, dated February 2003).

   B. Evaluated the current IRS Internal Revenue Manual, policies, procedures, and wireless guidance.

   C. Compared the IRS wireless policy and procedures to the Department of the Treasury, National Institute of Standards and Technology, and other Federal Government standards on wireless technology. We also compared them to private industry best practices and recommended solutions.

II. Evaluated the security of the ELITE wireless network.

   A. Reviewed approval documents to determine whether this wireless network was properly approved and whether the documents covered security concerns over wireless weaknesses.

   B. Evaluated system reviews conducted by the CSIRC and other organizations to identify whether problems with this wireless network have been previously identified.

   C. Evaluated the logical and physical security protections of this wireless network.

III. Determined whether any unauthorized wireless networks exist.

   A. Contacted IRS management, the CSIRC, and the Treasury Inspector General for Tax Administration System Intrusion Network Attack Response Team to determine the locations of known approved wireless networks and devices and how often scans for unapproved wireless services are performed, where these scans have been conducted, and what the results have been.

B. Remotely identified the number and types of wireless devices in use by performing a Nessus Access Point scan[1] of the entire IRS network.

C. Conducted 20 scans for wireless devices at a judgmental sample of IRS buildings in 10 different cities to identify unapproved wireless networks. The previous audit steps provided an indicator of wireless devices that may reside on the IRS network. This audit step was to determine the actual existences of the wireless devices. Selection of the sites we scanned was based on the locations of approved wireless systems, locations where wireless devices were identified in the past, and locations where wireless devices appeared to exist based on the scan in Step III.B. A judgmental sample was used because we were not planning to project our audit results. See Appendix IV for a list of the locations we scanned.

[1] Nessus is an open-source vulnerability assessment tool designed for Unix systems. In addition to identifying vulnerabilities in operating systems and applications, Nessus uses several techniques to identify unauthorized access point devices.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Acting Director
Thomas Polsfoot, Audit Manager
Esther Wilson, Lead Auditor
Charles Ekunwe, Senior Auditor
Cari Fogle, Senior Auditor
George Franklin, Senior Auditor
Jimmie Johnson, Senior Auditor
Louis Lee, Senior Auditor
Jackie Nguyen, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Chief Information Officer OS:CIO
- Chief, Mission Assurance and Security Services OS:MA
- Director, Program Oversight Office OS:CIO:SM:PO

Appendix IV

Locations Scanned for Wireless Devices

We scanned 20 offices in 10 cities to identify unapproved wireless devices. The table below presents the list of office locations we scanned and the number of devices identified.

Cities	Office Addresses	Unapproved Wireless Devices	
		Confirmed	Unconfirmed
Dallas, Texas	• 4050 Alpha Road		
	• 1100 Commerce Street		
Fort Worth, Texas	• 819 Taylor Street		
Houston, Texas	• 1919 Smith (Mickey Leland Building)		X
	• 8701 South Gessner		X
	• 12941 North IH-45		
	• 8876 Gulf Freeway		
Plantation, Florida	• 7850 Southwest 6th Court		X
	• 1000 South Pine Island Road		
Miami, Florida	• 51 Southwest First Avenue		
West Palm Beach, Florida	• 1700 Palm Beach Lakes Boulevard		
Denver, Colorado	• 600 17th Street	X	
	• 1244 Speer Boulevard		
Portland, Oregon	• 3rd Avenue (Federal Building)		
	• 120 Main Street		
Atlanta, Georgia	• 2970 Brandywine Road		
	• 401 West Peachtree Street		
	• 6655 Peachtree-Dunwoody Road		
	• 2888 Woodcock Boulevard		
Bloomington, Illinois	• 2402 East Empire (National Distribution Center)		
Totals: 10	**20**	**1**	**3**

Appendix V

Management's Response to the Draft Report

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

RECEIVED
MAR 2 0 2007

CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

MAR 1 9 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel Galik
Chief, Mission Assurance and Security Services

SUBJECT: Response to Draft Audit Report – Sensitive Data Remain at Risk From the Use of Unapproved Wireless Technology (Audit #200620029, I-trak #2007-21402)

Thank you for the opportunity to review the subject draft audit report, dated February 16, 2007. Wireless technology is among the security issues we are aggressively managing. The IRS has one authorized wireless network which we consider to be a low security risk. We are pleased that your report acknowledges IRS' Computer Security Incident Response Center conducted penetration tests of the wireless infrastructure and that we took immediate action to correct default configurations and to install a network intrusion prevention system for the wireless network.

We concur with the three report recommendations. Attached is a detailed response that outlines our corrective action plans for these recommendations. First, regarding wireless scanning activities, we initiated scans last year and we are expanding that monitoring capability. Next, to advise employees of wireless technology risks, we are using the security awareness program and training activities to disseminate information to IRS employees. Finally, actions are continuing to further manage wireless network configurations.

If you have any questions, please contact me at (202) 622-8910, or Devon Bryan, Director, IT Security at (202) 283-7271.

Attachment

Attachment

Management Response to Draft Audit Report – Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology (Audit # 200620029)

RECOMMENDATION #1:
The Chief, Mission Assurance and Security Services, should use available tools to proactively scan, on a continuous basis, the entire IRS network for unapproved wireless devices.

CORRECTIVE ACTION TO RECOMMENDATION #1:
Mission Assurance and Security Services established a wireless scanning project, and in November 2006, monthly scans were initiated at the nine campuses and three computing centers to determine whether unapproved wireless devices were present. Mission Assurance and Security Services will be expanding the number of locations to be scanned. A risk-based evaluation of the standard operating procedures (SOPs) will be performed to determine the additional sites that should be scanned and the SOPs will be updated as required.

IMPLEMENTATION DATE: December 15, 2007

RESPONSIBLE OFFICIAL: Director, IT Security, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN: Monthly reports are provided to the Director, IT Security, on the progress of all open corrective actions.

Attachment

Management Response to Draft Audit Report – Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology (Audit # 200620029)

RECOMMENDATION #2:
The Chief, Mission Assurance and Security Services, should periodically advise employees of the risk involved with wireless technology. The risk and consequences for violating the current wireless policy should also be included in annual security awareness training.

CORRECTIVE ACTION TO RECOMMENDATION #2:
Mission Assurance and Security Services will include information about the IRS wireless policy, risks associated with wireless technology, and the consequences of policy violations in the next annual mandatory security awareness training. In addition, Mission Assurance and Security Services will ensure that the IRS wireless technology policy and the wireless technology risks are a topic in the security awareness program for calendar year 2007.

IMPLEMENTATION DATE: January 15, 2008

RESPONSIBLE OFFICIAL: Director, IT Security, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN: Submission of content will be provided to the Director, Office of Privacy and Information Protection, for inclusion in annual Information Protection Briefing and in annual awareness strategy and plan.

Attachment

Management Response to Draft Audit Report – Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology (Audit # 200620029)

RECOMMENDATION #3:
The Chief Information Officer should ensure the Enterprise Networks Division takes appropriate action to monitor and track the configuration files on the ELITE wireless network to ensure all files are set in accordance with current policy.

CORRECTIVE ACTION TO RECOMMENDATION #3:

Enterprise Networks (EN) is working with Mission Assurance & Security Services' Computer Security Incident Response Center and the local End User Equipment & Services' Telecommunications staff to fully assess and manage the network devices in the Bloomington office, where the ELITE wireless network resides, to ensure that all router and switch configurations adhere to IRS Guidelines, Standards, and Procedures (GSP). The Bloomington site has both wired and wireless network components. All wired devices will be brought into the CiscoWorks and NetDoctor GSP Validation process. EN is obtaining an evaluation copy of CiscoWorks' Wireless LAN Solution to test its ability to manage the wireless devices in Bloomington. Wireless devices will be brought into the NetDoctor GSP Validation process.

IMPLEMENTATION DATE: June 1, 2008

RESPONSIBLE OFFICIAL: Acting Associate Chief Information Officer, Enterprise Networks, OS:CIO:EN

CORRECTIVE ACTION MONITORING PLAN: On a monthly basis until completion, the corrective action will be monitored through the Joint Audit Management Enterprise System (JAMES).