Use of Unapproved Wireless Technology
Puts Sensitive Data at Risk

February 2003

Reference Number: 2003-20-056

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.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

February 21, 2003

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Use of Unapproved Wireless Technology Puts Sensitive Data at Risk (Audit # 200220044)

This report presents the results of our review of the Internal Revenue Service's (IRS) use and security of wireless technology. The overall objective of this review was to determine the effectiveness of the IRS' actions to control and secure the use of wireless technology.

Wireless networks are rapidly gaining popularity in the Federal Government and private sectors because they are inexpensive and provide greater flexibility than wired networks. With the advantages come security vulnerabilities, particularly with unauthorized disclosure of sensitive data. Before a wireless network is implemented, the advantages need to be carefully weighed against the vulnerabilities.

The IRS recognized the risks when its limited scanning in the Washington, D.C., area from December 2001 to March 2002 identified three unexpected wireless networks. Although these wireless applications were shut down, over 6 months passed before the IRS initiated comprehensive efforts to identify other applications and educate all employees about the risks of using wireless technologies.

In summary, our subsequent scanning identified an unauthorized wireless application in one location that was directly connected to the IRS-wide internal network containing sensitive taxpayer information. Although encryption was used, the encryption key was unchanged for 2 years and could have been compromised. We were able to capture traffic from this application from a hotel approximately one-quarter mile away from the IRS building. The IRS advised us that this application had no current business purpose.

At a second location, we had strong indications of another wireless application. However, we were unable to confirm the existence of the wireless components and configurations of the wireless application because the wireless signal was abruptly terminated when we entered this location and advised the employees in the office of our review.

In addition, we identified the potential for unauthorized disclosure of sensitive data on the approved wireless application supporting the IRS' Continuity of Operation Plan (COOP). The IRS has authorized the use of wireless devices for executives in the event of an emergency and has configured the supporting network to ensure that all transmissions are encrypted. However, once electronic mail messages are read on the wireless devices, the messages are stored unencrypted.

We recommended that the Deputy Commissioner for Modernization & Chief Information Officer immediately disconnect all unapproved wireless networks that are connected to the IRS architecture, incorporate policies and procedures for the use of wireless technology into the segment of the Internal Revenue Manual (IRM) addressing Information Technology Security Policies and Guidance, and ensure wireless scanning efforts include critical assets. Also, we recommended that action be taken to minimize the exposure of unencrypted sensitive data stored on the wireless devices supporting the COOP.

Management's Response: The Chief, Security Services, concurred with the findings in this report and has taken actions to address the security vulnerabilities associated with wireless networks. Specifically, the IRS has terminated all known unapproved wireless networks connected to the internal network, incorporated the topic of wireless technology in the IRM, conducted and will continue to conduct unannounced scans for wireless networks, and taken steps to address unencrypted sensitive data on wireless devices for the COOP. 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 who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs), at (202) 927-7291.

Table of Contents

Background

Wireless[1] networks are rapidly gaining popularity in the Federal Government and private sectors because they are inexpensive (a wireless network can be set up for less than $250). Wireless networks also provide greater flexibility. For example, when an office is moved, wires do not need to be restrung through walls.

Wireless technology is based on sending radio-wave transmissions through the air between two points, usually a user laptop computer and a pre-defined access point. The access point can be connected back to the organization's network to allow for full functionality and access to all computer resources.

With the advantages associated with wireless networks come significant security risks. 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. Anyone can obtain free software from the Internet to break this encryption. In addition, the existence of a wireless access point represents another avenue into an organization's network infrastructure.

Recent commercial incidents have also demonstrated some of the vulnerabilities of wireless networks. For example, one large retailer was using unencrypted wireless to transmit cash register transactions. These transactions contained customer credit card numbers and other sensitive information. The transmissions were shut down after someone sitting in the parking lot intercepted the transactions and reported it to the company.

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 buildings housing insecure wireless networks for others to potentially exploit.

Federal Government agencies are aware of the wireless vulnerabilities and have responded accordingly. For

[1] For this report, wireless is defined as IEEE 802.11b - 2.4 GHz frequencies.

example, the United States Secretary of Defense has placed a moratorium on the installation of telecommunications network infrastructure to support wireless services in the Pentagon area. The Secret Service has initiated an effort to identify and report insecure wireless activities in the Washington, D.C., metropolitan area.

For the Internal Revenue Service (IRS), the security risks associated with wireless technology mainly involve the improper access to and unauthorized disclosure of sensitive data. Sensitive financial data for over 130 million taxpayers could be at risk.

The audit was conducted from July through November 2002 in IRS offices located in Washington, D.C.; Oakland, Sacramento, San Francisco, and San Jose, California; Las Vegas, Nevada; Memphis, Tennessee; and Dallas, Texas. The audit was conducted in accordance with *Government Auditing Standards.* Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Timely Actions Were Not Taken to Eliminate Unauthorized Wireless Networks

We scanned IRS buildings in eight cities using inexpensive wireless equipment and software freely available on the Internet. We identified an unapproved wireless application in one location and had strong indications of another wireless application in a second location.

The Information Technology Services organization in one office connected its wireless application to the internal IRS-wide network. Not only were data on the wireless network exposed in this instance, but sensitive taxpayer data and systems on the entire IRS network were vulnerable. The IRS advised us that the application had no current business purpose.

We were able to capture traffic from this application from a hotel approximately one-quarter mile away from the IRS building. Either a hacker or occupants in nearby buildings could have easily captured the IRS' wireless traffic. The wireless traffic in this case was encrypted. However, with free software available on the Internet, they could have cracked the encryption key[2] in a short time, obtained passwords, and accessed the IRS network.

Encryption keys should be changed regularly and often to minimize the opportunities for hackers to gather sufficient information to crack the keys. However, the encryption key for this wireless application had not been changed for 2 years.

At another location, we identified an encrypted wireless signal and were able to isolate the signal to a specific IRS office. However, we were unable to confirm the existence of the wireless components and configurations of the wireless application. The wireless signal was abruptly terminated immediately after we arrived in the office and informed employees of our purpose. We made an unannounced return visit and did not find the wireless application active.

Discussions with numerous IRS managers and employees showed they did not understand or were not aware of the security vulnerabilities associated with wireless technology. Only the Information Technology Services employees seemed to generally understand the risks with wireless technology and the IRS' position not to deploy it.

Documentation shows that IRS security officials have been aware of the risks associated with wireless technology for over a year. From November 2001 through March 2002, the IRS' Computer Security Incident Response Center (CSIRC) and Treasury Inspector General for Tax Administration's System Intrusion Network Attack Response Team (SINART) jointly conducted scans for wireless technology at selected IRS facilities in the Washington, D.C., area. These scans identified three unexpected applications, which were subsequently shut down.

Because of the potential security vulnerability of wireless applications, the CSIRC and SINART jointly issued a memorandum on March 20, 2002, to the Director of

[2] An encryption key is a binary number, typically from 40 to 128 bits in length, and is mathematically combined with plaintext data to produce encrypted data. The key is also used to decode the encrypted data back to plaintext.

Cyber-Security (now the Director, Mission Assurance) discussing their results. In addition, they made recommendations to create a more secure communication channel for wireless use or disallow connectivity to the IRS' internal network. They also suggested that a review of the current IRS policy be conducted for adequate wireless security consideration.

Approximately 6 months after the issuance of the memorandum, the IRS' Technology Security Committee approved the release of a wireless article through publication channels for issuance throughout the IRS. This article stated that any use of wireless technology needs to be approved by the Office of Security Services, and it prohibited the use of wireless devices without a security certification and accreditation. The IRS distributed this article by posting it on the Security Services Intranet web site in October 2002 and including it in a November 2002 all employee newsletter, *IRS Headlines… and More*. The IRS has also initiated actions to have one of its contractors conduct wireless scans at various IRS locations during Fiscal Year 2003.

We are encouraged by these activities. They provide greater awareness of wireless security vulnerabilities and a means to identify unauthorized use. The IRS is no longer relying on its general security policy and has issued specific guidance regarding the use of wireless technology. We concur with the approach for developing technology-specific guidance as appropriate and necessary.

Recommendations

The Deputy Commissioner for Modernization & Chief Information Officer (CIO) should:

1. Immediately shut down all known wireless applications connected to the IRS architecture that have not gone through the proper approval process and security evaluations.

Management's Response: The IRS shares our concerns with employees connecting wireless devices to the internal network. All known unapproved wireless applications connected to the IRS architecture have been terminated.

2. Incorporate the policies, procedures, and guidance developed for the use of wireless technology into the Internal Revenue Manual (IRM).

Management's Response: IRS policies and procedures covering network connectivity, including wireless network connectivity, are currently reflected in the IRM.

3. Ensure wireless scanning efforts include sufficient geographical coverage to provide representative assessments of unapproved wireless use.

Management's Response: The IRS has increased coverage on wireless scanning through an inter-agency agreement with one of its contractors. In addition, the IRS' CSIRC has augmented its activities to perform random on-going unannounced wireless scans at IRS sites on an enterprise-wide basis.

Additional Actions Could Be Taken to Protect Sensitive Data Stored on Approved Wireless Devices

The IRS has approved the use of wireless technology for its Continuity of Operation Plan (COOP) and CSIRC. Approximately 300 wireless devices were obtained for executives and other key personnel and are to be used to transmit emergency and computer security communications. In addition, the employees can remotely access their desktop electronic mail (email) messages using the devices, depending on how the employee sets the rules as to what is forwarded to the device.

The wireless application securely transmits the email messages using a Federal Government-approved encryption method. The information is encrypted from the internal server to the device. The IRS also uses strong passwords and screen saver lockout features to help secure the information stored on the devices.

However, once email messages are read on the device, the information is stored unencrypted. The user guide for the device does not mention this, and users may not be aware that they need to delete the email messages after reading them. Because these devices are small and portable, they can easily be lost or stolen. Any unencrypted information would thereby be at risk of disclosure.

Recommendation

4. The Deputy Commissioner for Modernization & CIO should minimize the exposure of sensitive data stored on the wireless devices by completing one of the following actions:

    - Encrypt all data stored on the wireless devices.
    - Incorporate restrictive rules on forwarding email messages to the devices.
    - Advise users to delete sensitive emails after reading them.

Management's Response: The IRS will implement Secure/Multipurpose Internet Mail Extensions protocol messaging to wireless messaging devices. This will provide IRS employees the ability to securely handle all sensitive message traffic to wireless devices, including the storage of encrypted messages on the devices. In addition, the IRS will implement an aggressive re-education program to ensure that all employees are aware of how to identify and protect sensitive information and to use secure messaging.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of the Internal Revenue Service's (IRS) actions to control and secure the use of wireless technology.

I. To assess the current IRS position regarding the use of wireless technology, we:

   A. Reviewed the Department of the Treasury, IRS, and other appropriate guidance documents related to establishing the use of wireless technology.

   B. Determined IRS management's responsibilities for wireless technology.

II. To evaluate the security of approved wireless applications, we:

   A. Reviewed approval documents, including certifications, schematics, and operating plans.

   B. Evaluated the logical security protections, including the use of encryption.

III. To identify any unauthorized use of wireless technology, we:

   A. Specifically configured a laptop computer to receive wireless transmissions and scanned for the existence of wireless access points in IRS offices located in Washington, D.C.; Oakland, Sacramento, San Francisco, and San Jose, California; Las Vegas, Nevada; Memphis, Tennessee; and Dallas, Texas.

   B. Recorded transmissions and reviewed them to ensure they were IRS-related.

   C. Attempted to exploit any wireless applications inter-connected to the IRS architecture.

IV. To determine the level of employee awareness regarding the use of wireless technology and determine actions taken to educate employees, we:

   A. Identified any policy or guidance documents and their distribution.

   B. Discussed the use of wireless technology with managers and employees at seven of the eight locations visited.

   C. Discussed employee training and awareness regarding wireless technology with the Office of the Deputy Commissioner for Modernization & Chief Information Officer, the Business Unit Division Information Officers, and other appropriate entities.

   D. Reviewed any employee alerts, messages, etc., pertaining to wireless technology.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Harry Dougherty, Senior Auditor
Louis Lee, Senior Auditor
Larry Reimer, Senior Auditor
William Simmons, Auditor

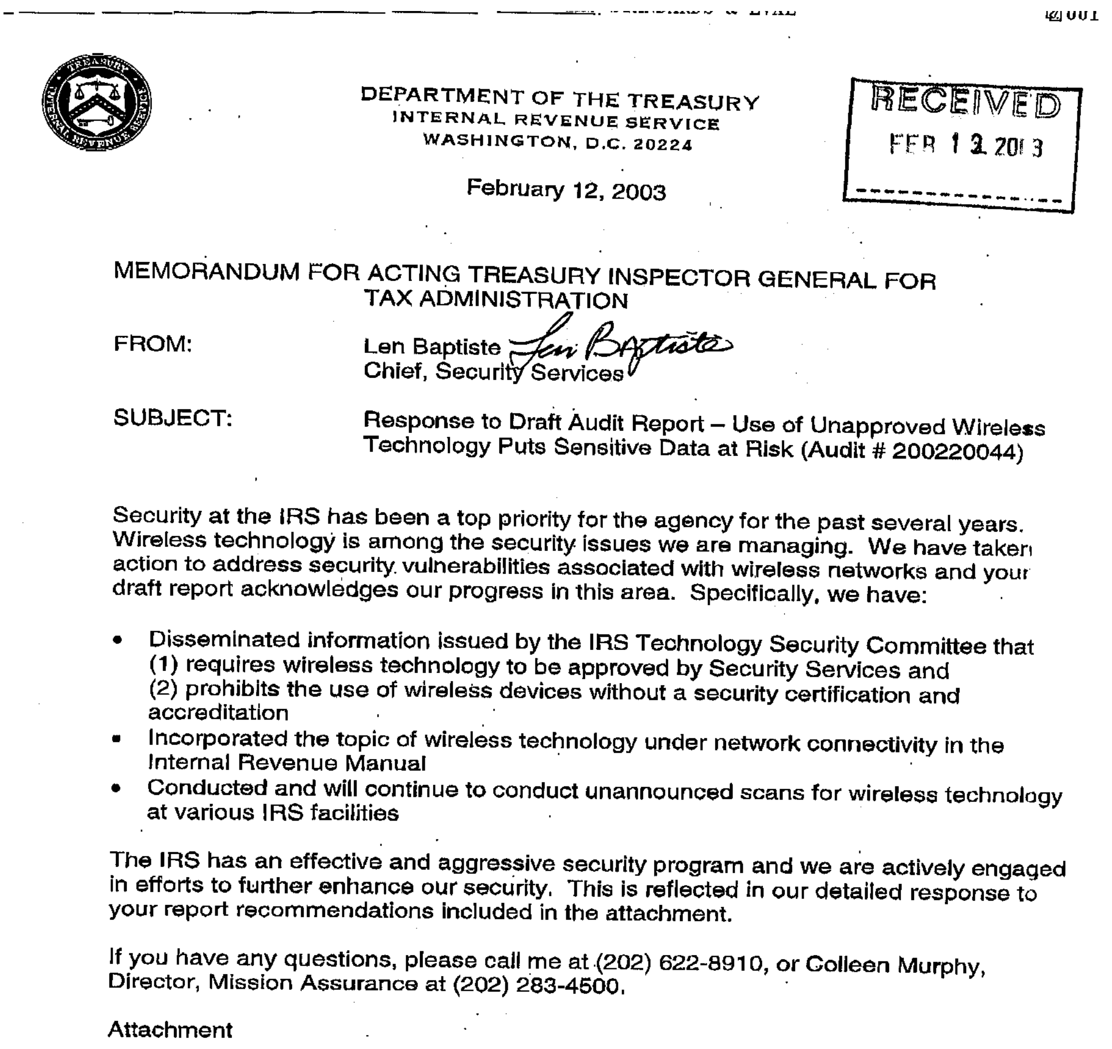
Appendix III

Report Distribution List

Acting Commissioner N:C
Chief, Information Technology Services M:I
Chief, Security Services M:S
Director, Mission Assurance M:S:A
Deputy Director, Computer Security Incident Response Capability M:S:A:IR
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons:
    Deputy Commissioner for Modernization & Chief Information Officer M
    Chief, Security Services M:S

Appendix IV

Management's Response to the Draft Report



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

February 12, 2003

MEMORANDUM FOR ACTING TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Len Baptiste Len Baptiste
Chief, Security Services

SUBJECT: Response to Draft Audit Report – Use of Unapproved Wireless Technology Puts Sensitive Data at Risk (Audit # 200220044)

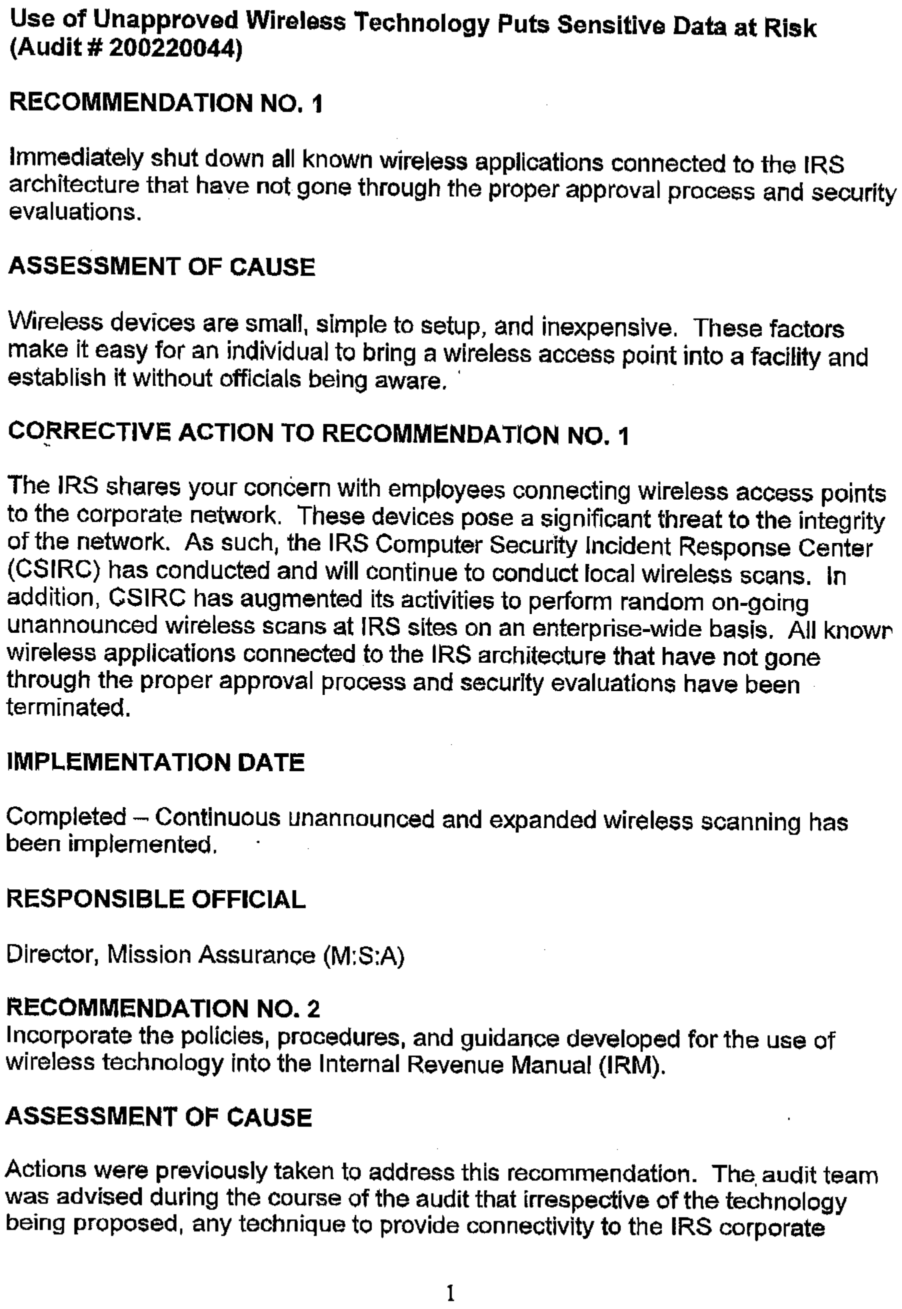
Security at the IRS has been a top priority for the agency for the past several years. Wireless technology is among the security issues we are managing. We have taken action to address security vulnerabilities associated with wireless networks and your draft report acknowledges our progress in this area. Specifically, we have:

- Disseminated information issued by the IRS Technology Security Committee that (1) requires wireless technology to be approved by Security Services and (2) prohibits the use of wireless devices without a security certification and accreditation
- Incorporated the topic of wireless technology under network connectivity in the Internal Revenue Manual
- Conducted and will continue to conduct unannounced scans for wireless technology at various IRS facilities

The IRS has an effective and aggressive security program and we are actively engaged in efforts to further enhance our security. This is reflected in our detailed response to your report recommendations included in the attachment.

If you have any questions, please call me at (202) 622-8910, or Colleen Murphy, Director, Mission Assurance at (202) 283-4500.

Attachment



Use of Unapproved Wireless Technology Puts Sensitive Data at Risk (Audit # 200220044)

RECOMMENDATION NO. 1

Immediately shut down all known wireless applications connected to the IRS architecture that have not gone through the proper approval process and security evaluations.

ASSESSMENT OF CAUSE

Wireless devices are small, simple to setup, and inexpensive. These factors make it easy for an individual to bring a wireless access point into a facility and establish it without officials being aware.

CORRECTIVE ACTION TO RECOMMENDATION NO. 1

The IRS shares your concern with employees connecting wireless access points to the corporate network. These devices pose a significant threat to the integrity of the network. As such, the IRS Computer Security Incident Response Center (CSIRC) has conducted and will continue to conduct local wireless scans. In addition, CSIRC has augmented its activities to perform random on-going unannounced wireless scans at IRS sites on an enterprise-wide basis. All knowr wireless applications connected to the IRS architecture that have not gone through the proper approval process and security evaluations have been terminated.

IMPLEMENTATION DATE

Completed – Continuous unannounced and expanded wireless scanning has been implemented.

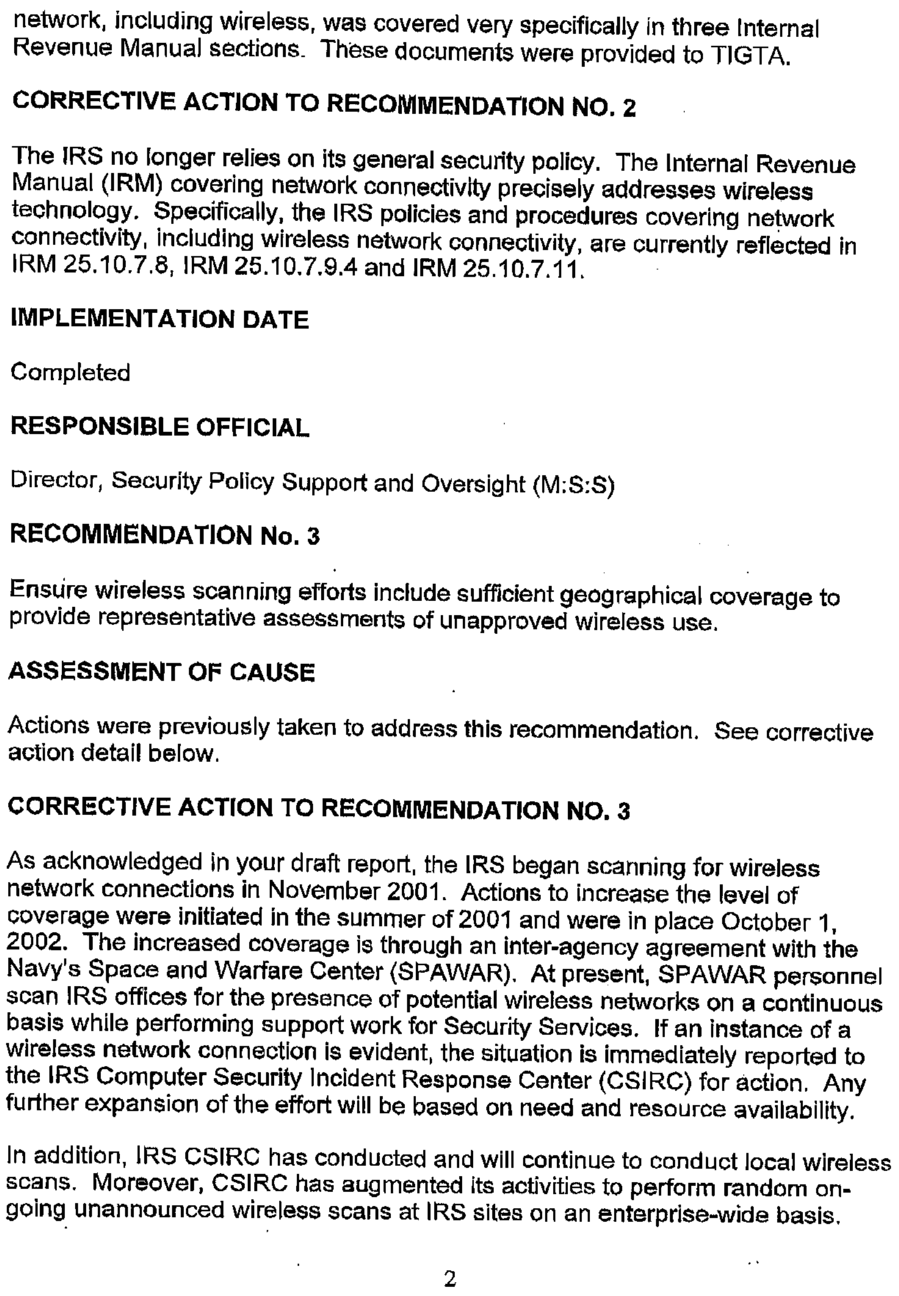
RESPONSIBLE OFFICIAL

Director, Mission Assurance (M:S:A)

RECOMMENDATION NO. 2
Incorporate the policies, procedures, and guidance developed for the use of wireless technology into the Internal Revenue Manual (IRM).

ASSESSMENT OF CAUSE

Actions were previously taken to address this recommendation. The audit team was advised during the course of the audit that irrespective of the technology being proposed, any technique to provide connectivity to the IRS corporate



network, including wireless, was covered very specifically in three Internal Revenue Manual sections. These documents were provided to TIGTA.

CORRECTIVE ACTION TO RECOMMENDATION NO. 2

The IRS no longer relies on its general security policy. The Internal Revenue Manual (IRM) covering network connectivity precisely addresses wireless technology. Specifically, the IRS policies and procedures covering network connectivity, including wireless network connectivity, are currently reflected in IRM 25.10.7.8, IRM 25.10.7.9.4 and IRM 25.10.7.11.

IMPLEMENTATION DATE

Completed

RESPONSIBLE OFFICIAL

Director, Security Policy Support and Oversight (M:S:S)

RECOMMENDATION No. 3

Ensure wireless scanning efforts include sufficient geographical coverage to provide representative assessments of unapproved wireless use.

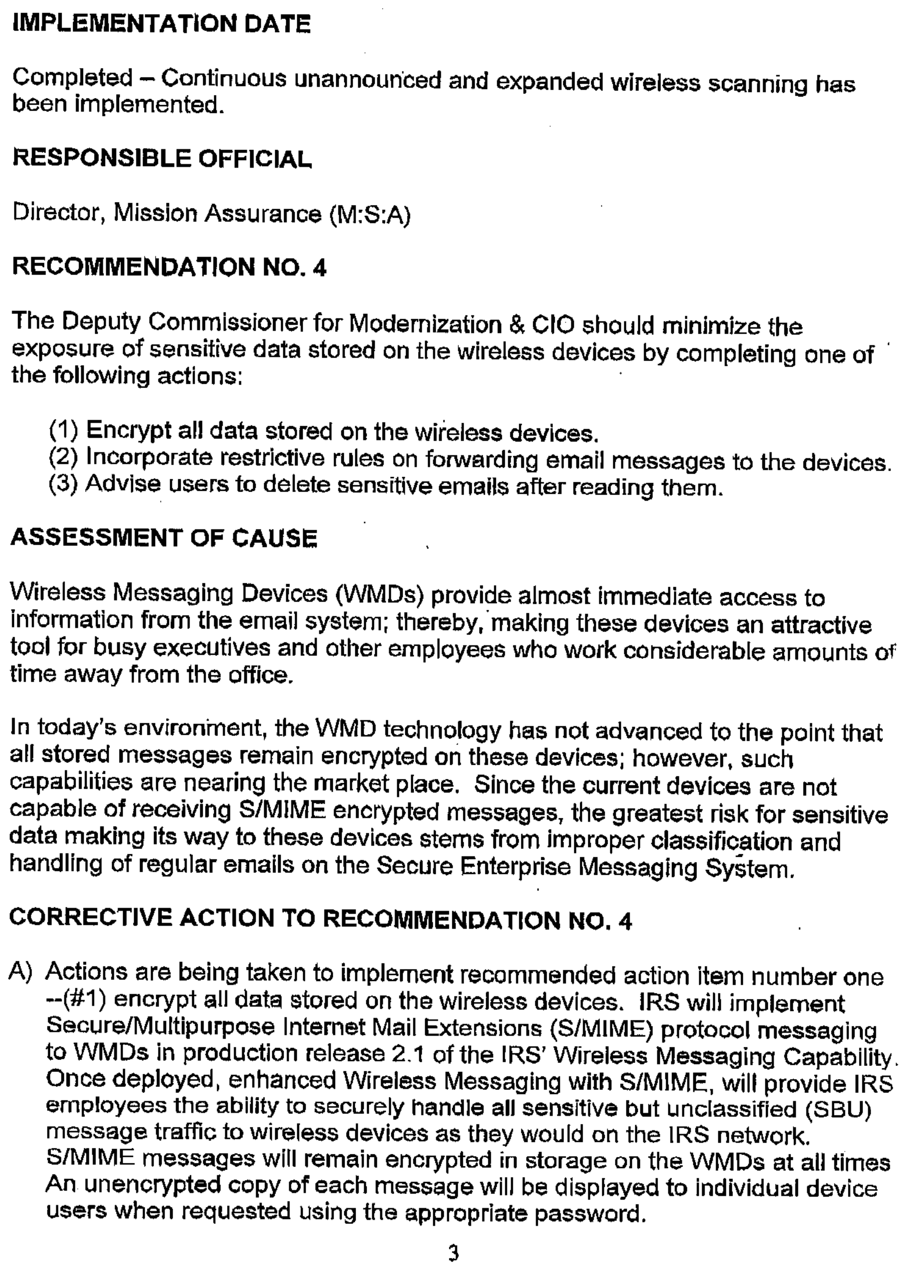
ASSESSMENT OF CAUSE

Actions were previously taken to address this recommendation. See corrective action detail below.

CORRECTIVE ACTION TO RECOMMENDATION NO. 3

As acknowledged in your draft report, the IRS began scanning for wireless network connections in November 2001. Actions to increase the level of coverage were initiated in the summer of 2001 and were in place October 1, 2002. The increased coverage is through an inter-agency agreement with the Navy's Space and Warfare Center (SPAWAR). At present, SPAWAR personnel scan IRS offices for the presence of potential wireless networks on a continuous basis while performing support work for Security Services. If an instance of a wireless network connection is evident, the situation is immediately reported to the IRS Computer Security Incident Response Center (CSIRC) for action. Any further expansion of the effort will be based on need and resource availability.

In addition, IRS CSIRC has conducted and will continue to conduct local wireless scans. Moreover, CSIRC has augmented its activities to perform random on-going unannounced wireless scans at IRS sites on an enterprise-wide basis.



IMPLEMENTATION DATE

Completed – Continuous unannounced and expanded wireless scanning has been implemented.

RESPONSIBLE OFFICIAL

Director, Mission Assurance (M:S:A)

RECOMMENDATION NO. 4

The Deputy Commissioner for Modernization & CIO should minimize the exposure of sensitive data stored on the wireless devices by completing one of the following actions:

(1) Encrypt all data stored on the wireless devices.
(2) Incorporate restrictive rules on forwarding email messages to the devices.
(3) Advise users to delete sensitive emails after reading them.

ASSESSMENT OF CAUSE

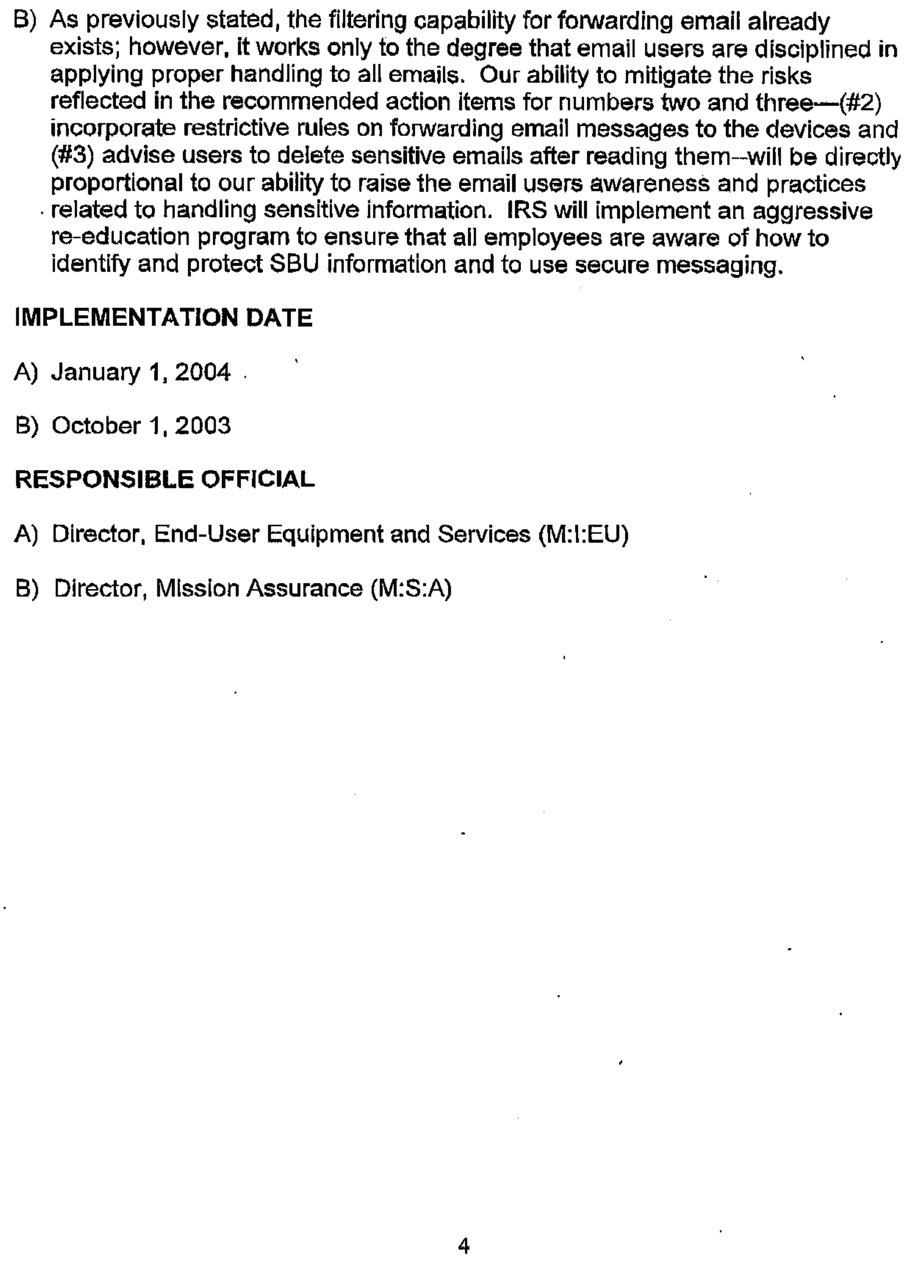
Wireless Messaging Devices (WMDs) provide almost immediate access to information from the email system; thereby, making these devices an attractive tool for busy executives and other employees who work considerable amounts of time away from the office.

In today's environment, the WMD technology has not advanced to the point that all stored messages remain encrypted on these devices; however, such capabilities are nearing the market place. Since the current devices are not capable of receiving S/MIME encrypted messages, the greatest risk for sensitive data making its way to these devices stems from improper classification and handling of regular emails on the Secure Enterprise Messaging System.

CORRECTIVE ACTION TO RECOMMENDATION NO. 4

A) Actions are being taken to implement recommended action item number one --(#1) encrypt all data stored on the wireless devices. IRS will implement Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol messaging to WMDs in production release 2.1 of the IRS' Wireless Messaging Capability. Once deployed, enhanced Wireless Messaging with S/MIME, will provide IRS employees the ability to securely handle all sensitive but unclassified (SBU) message traffic to wireless devices as they would on the IRS network. S/MIME messages will remain encrypted in storage on the WMDs at all times An unencrypted copy of each message will be displayed to individual device users when requested using the appropriate password.

3



B) As previously stated, the filtering capability for forwarding email already exists; however, it works only to the degree that email users are disciplined in applying proper handling to all emails. Our ability to mitigate the risks reflected in the recommended action items for numbers two and three—(#2) incorporate restrictive rules on forwarding email messages to the devices and (#3) advise users to delete sensitive emails after reading them--will be directly proportional to our ability to raise the email users awareness and practices related to handling sensitive information. IRS will implement an aggressive re-education program to ensure that all employees are aware of how to identify and protect SBU information and to use secure messaging.

IMPLEMENTATION DATE

A) January 1, 2004

B) October 1, 2003

RESPONSIBLE OFFICIAL

A) Director, End-User Equipment and Services (M:I:EU)

B) Director, Mission Assurance (M:S:A)