Security Over Computers Used in Telecommuting Needs to Be Strengthened

July 2003

Reference Number: 2003-20-118

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 1, 2003

MEMORANDUM FOR ACTING DEPUTY COMMISSIONER FOR MODERNIZATION & CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and Corporate Programs)

SUBJECT: Final Audit Report - Security Over Computers Used in Telecommuting Needs to Be Strengthened (Audit # 200220031)

This report presents the results of our review to evaluate actions taken by the Internal Revenue Service (IRS) to reduce the risks associated with telecommuting. The Congressional Federal Telework Mandate 2001[1] required executive agencies to establish policies that enable eligible employees to participate in telecommuting. While telecommuting provides benefits for both the Federal Government and its employees, certain security risks must be addressed. IRS employees who work away from the traditional office must safeguard taxpayer data on their laptop computers and securely transmit data back to the office. In addition, we conducted this review in response to an inquiry from Senator Charles E. Grassley, then Ranking Member of the Senate Committee on Finance, who requested that we assess the sufficiency of IRS encryption practices to prevent unauthorized disclosure of taxpayer information when a computer is lost or stolen.

In summary, sensitive data on laptop computers were vulnerable to unauthorized disclosure. Employees did not always encrypt files as required by the IRS, and the encryption method used on some laptop computers did not comply with Federal Government standards. To compound these issues, improper security settings on laptop computers allowed password controls to be bypassed. As a result, a thief with minimal hacking skills could steal an IRS laptop computer and easily gain access to sensitive data.

[1] Department of Transportation Appropriation Act of 2001, Pub. L. No. 106-346, Section 359 (2000).

The IRS has provided a secure infrastructure for its employees to connect to the network. All transmissions, when properly done, were encrypted. However, the IRS could enhance the security of the architecture supporting employees working away from the office. Specifically, firewall systems protecting the main servers were not consistently set up and updated as the computer industry identified security vulnerabilities. Also, firewall and intrusion detection system software was not installed on all laptop computers.

To address laptop computer security weaknesses, we recommended that the Acting Deputy Commissioner for Modernization & Chief Information Officer (CIO):

- Provide increased security awareness for employees.
- Develop guidance for functional managers to ensure sensitive data on laptop computers are encrypted.
- Require that encryption keys for laptop computers be kept separate from hard drives.
- Give consideration to encryption packages that comply with Federal Government requirements.

We also recommended that the Commissioners of the Large and Mid-Size Business, Small Business/Self-Employed, and Tax Exempt and Government Entities Divisions, and the Chief, Agency-Wide Shared Services, require first-line managers to periodically check employees' laptop computers to ensure that sensitive data are encrypted. To address security enhancements on the computer architecture supporting telecommuters and the mobile workforce, we recommended correcting firewall system issues and giving consideration to installing personal firewall and intrusion detection system software on all laptop computers.

Management's Response: IRS management agreed with most of our recommendations. To address laptop computer security weaknesses, the Acting Deputy Commissioner for Modernization & CIO will send out periodic reminders to employees and system administrators of their laptop security responsibilities, and will conduct research for compliant replacement technology for the current file encryption solutions. To address architecture security weaknesses, the Acting Deputy Commissioner for Modernization & CIO will take actions to timely patch firewall software and implement the Enterprise Remote Access Project, which will provide for personal firewall protection and intrusion detection capabilities for all computers that access the IRS network remotely.

The IRS partially concurred with our recommendations on requiring functional managers to check employee laptops for encryption of sensitive data. While IRS management agreed that employees should comply with encryption steps to safeguard data on laptop computers, they believe that IRS security professionals, rather than front-line managers, should review laptop computers for noncompliance. The IRS did not agree with our recommendation about keeping encryption keys separate from the hard drives. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We do not believe that merely asking the security professionals to review a sample of laptop computers will ensure encryption of sensitive data. While we recognize the many demands on front-line managers, periodically reviewing employees' laptops to ensure proper encryption should be considered an integral responsibility for managers and should not be difficult or time-consuming. Also, even though management has decided to accept the risk of not maintaining encryption keys separate from hard drives, we continue to believe it is prudent to keep them separate. While we still believe our recommendations are worthwhile, we do not intend to elevate our disagreement concerning them to the Department of the Treasury for resolution.

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

Table of Contents

Background

The Internal Revenue Service (IRS) has moved toward allowing more and more of its employees to work away from the traditional office. This is, in part, because of the Congressional Federal Telework Mandate 2001,[1] which required executive agencies to establish policies under which eligible employees may participate in telecommuting. While telecommuting provides benefits to both the Federal Government and its employees, there are related security risks that must be addressed.

The security risks of telecommuting in the IRS involve the protection of taxpayer data. Working away from the office is not a new concept at the IRS. IRS employees have always conducted official business on taxpayer property, particularly with businesses and large corporations. These employees are required to safeguard taxpayer information, whether it is on their laptop computers, external media, or hardcopy documents.

Laptop computers pose a significant risk because they are easily lost or stolen. Over one-half of the 23 laptops reported stolen from December 2001 to July 2002 had been left unattended in personal vehicles for longer than necessary. At least 10 of them probably contained sensitive data.

In a letter to the Treasury Inspector General for Tax Administration (TIGTA) dated January 9, 2002, Senator Charles E. Grassley, then Ranking Member of the Senate Committee on Finance, expressed concerns over lost or stolen sensitive items of inventory at the IRS. In his request, he asked that the TIGTA assess the sufficiency of IRS encryption[2] practices to prevent the unauthorized disclosure of taxpayer information when a computer is lost or stolen.

---

[1] Department of Transportation Appropriation Act of 2001, Pub. L. No. 106-346, Section 359 (2000).

[2] Encryption is defined as the reversible transformation of data from the original (i.e., plaintext) to a difficult-to-read format (i.e., ciphertext) as a mechanism for protecting its confidentiality, integrity, and sometimes its authenticity. Encryption uses an algorithm and one or more encryption keys to make the conversion.

We conducted a review and issued a Management Advisory Report[3] that stated some of the laptops tested did not have encryption software installed, while others that did have encryption software installed contained unencrypted taxpayer information. Because a very limited sample was selected, we decided to perform a more thorough review to determine the extent to which the IRS is at risk of unauthorized disclosure of taxpayer information.

There is another security risk with employees working away from the office. With the creation of home offices and the continuing use of permanent offices at taxpayer locations, the IRS has to provide its employees with the means to connect to its network from the outside while maintaining security over these connections. Consequently, it is critical that the IRS has adequate information technology architectures to support the employees' needs as well as the agency's security concerns.

There are currently two methods to allow employees to connect to the IRS network. First, Secure Dial-In (SDI)[4] allows most employees to connect to the IRS network via telephone lines. By the end of Fiscal Year 2003, the IRS estimates over 30,000 employees will have laptop computers with SDI capabilities. Second, the Large and Mid-Size Business Division has started a Virtual Private Network (VPN)[5] pilot for its employees at its larger taxpayer businesses. The pilot consists of 32 sites, which ranged from 3 employees at the smallest site to 43 employees at the largest site.

The audit was conducted from July 2002 through March 2003 in the IRS' offices in Baltimore, Chicago,

---

[3] *Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service* (Reference Number 2002-10-065, dated March 2002).

[4] SDI consists of computer hardware and software that allows an organization to make secure remote connections through a toll-free telephone line to the organization's internal network.

[5] Similar to SDI, a VPN consists of computer hardware and software that allow an organization to securely communicate through the Internet or a set of local telephone lines. It establishes an encrypted "tunnel" for connections to an organization's internal network.

Detroit, and Washington, D.C., and in the Detroit and Martinsburg Computing Centers.[6] 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.

Sensitive Data on Laptop Computers Were Vulnerable to Unauthorized Disclosure

The IRS established adequate security policies and procedures for employees working away from the office. Incident reporting ensured that actions were taken to limit the exposure to loss when laptop computers were lost or stolen.

To prevent disclosure of sensitive information on lost or stolen laptop computers, the IRS requires that all sensitive files be encrypted and that access to the laptops be controlled by the use of passwords. However, these procedures were not properly implemented. Employees did not always encrypt files and, in many instances, the encryption used was weak and did not comply with Federal Government standards. All laptops were protected by passwords; however, the password controls could be circumvented.

As a result of the weaknesses we identified, a thief with minimal hacking skills could steal an IRS computer and easily gain access to sensitive data.

Sensitive files were not adequately encrypted

Of 105 laptop computers we sampled, 32 (30 percent) stored unencrypted confidential information – 26 with taxpayer data and 6 with IRS employee personnel records. Examples of the unencrypted files include: taxpayers' bank reconciliations, innocent spouse documents, a list of employees with contribution amounts to a political action committee, and employee evaluations.

The IRS has defined directories on the hard drive where sensitive data are required to be stored and encrypted. We found that employees frequently placed sensitive data outside of those directories, either because the employees

[6] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

were not aware of the security requirements or for their convenience.

Encryption software had not been installed or it had been installed improperly on 12 of the 73 laptops that did not contain sensitive information. Since these laptops can be used for future telecommuting, the encryption software should have been installed.

In addition, the encryption key for laptop computers used in the VPN pilot was improperly stored on the computers' hard drives. Since the encryption key is needed to decrypt data, the key must be kept separate from the data. IRS procedures recognize this and cite the need for strong key management. The National Institute of Standards and Technology (NIST) also recognized the importance of key storage and encryption when it states, "…that even if an attacker compromises a host via a remote attack or is in physical possession of the media, they will be unable to read the encrypted data, provided the keys are not stored on the system."[7]

The IRS did not consider the risks of storing the key on the laptop computer. If an experienced hacker were to steal one of these laptops, he or she could use readily available tools from the Internet to determine valid user accounts and ascertain the passwords for any user accounts stored on the computer. The hacker would then be able to log onto the computer as the employee and decrypt all of the encrypted files using the locally stored encryption key.

Finally, the encryption scheme for some laptop computers was DESX, which is not compliant with the Federal Information Processing Standard (FIPS) 140-2[8] and not one of the encryption schemes recommended by the NIST. These laptop computers have the Microsoft Windows 2000 operating system, which does not normally come with a FIPS-compliant encryption scheme. The IRS elected to use

---

[7] NIST Special Publication 800-46: *Security for Telecommuting and Broadband Communications*.

[8] FIPS 140-2, Security Requirements for Cryptographic Modules (issued May 25, 2001), presents and explains encryption standards to be used within the Federal Government.

the encryption package provided by Windows 2000 for convenience. However, using a noncompliant encryption solution is a violation of Federal Government security guidelines.

Not having encryption and not properly storing encryption keys make the data on laptop computers more easily accessible to unauthorized persons. The significance of these conditions is greatly increased by the configuration weaknesses detailed in the following section.

Password controls over laptop computers could be easily circumvented

To prevent unauthorized access to programs and files maintained on IRS laptop computers, the IRS makes use of an operating system password access control. By using this method, a person must have a system-recognized logon name and password to gain access to the computer.

All laptop computers in our sample were protected by the operating system password access control. However, we identified security configuration weaknesses that allow anyone with physical access to the laptop computer to bypass this up-front password access control.

Of 105 laptops computers we sampled, 44 (42 percent) would boot[9] from a removable media drive.[10] The 44 laptop computers consisted of 33 that were configured that way and 11 that were configured with no password protecting the boot order. IRS policies and procedures require that all computers boot only from the internal hard drive. The boot order password is also required to be enabled so that only authorized personnel, usually system administrators, can change the boot order.

When a computer will boot up from the removable media drive, a hacker can bypass all security controls established on the computer's operating system, including the password access control. In addition, when no password is enabled to

[9] The term "boot" represents the automatic start-up process when the computer is turned on. A computer usually boots from its hard drive.

[10] A removable media drive is the disk drive where a 3 ½" diskette or a CD-ROM disk can be inserted to access software programs or data.

protect the boot order, a hacker can interrupt the computer's normal start-up sequence and change the boot order so that the first drive the computer accesses is the removable media drive.

For example, a hacker could insert a diskette or CD-ROM containing another operating system program and turn on the laptop. If the laptop computer is allowed to boot up from removable media drives, the laptop will start up with the operating system on the diskette or CD-ROM instead of the one installed on the hard drive. The hacker will now have access to all of the data on the hard drive, which makes proper encryption of sensitive data that much more important.

Of the 44 laptop computers with external bootable drives or where the password protecting the boot order was disabled, 18 contained unencrypted sensitive files. If these laptops were lost or stolen, anyone following the steps above could easily bypass all security logon controls and access sensitive taxpayer data.

We also found that 13 of the 105 laptop computers sampled had additional accounts established which improperly allowed the user administrative rights. Users with administrative rights could modify or disable the security settings, including the way encryption works.

In addition, the laptop computers were set to locally save the logon credentials for the previous 10 employees who logged onto the laptop. The saved logon credentials will allow these employees to access the laptop computer when it is not connected to the network. This is an acceptable practice in an office environment where computer workstations are shared among numerous employees. However, in a telecommuting environment where a laptop is assigned to 1 employee, saving up to 10 user profiles poses an unnecessary risk.

If the laptop computer were stolen, the thief could identify one of the user accounts and then crack the password using publicly available hacking software. The thief could use this information to gain access to the IRS network and other computer resources. System administrators would find it difficult to determine whose user accounts and passwords

had been saved on the laptop computer. These accounts would have to be identified so that the system administrators can deactivate the network user accounts or change the network passwords to prevent misuse.

Because our review represents a snapshot of the security configurations on the laptop computers, it was difficult to determine when, how, or why the security settings were changed. Discussions with field personnel yielded one feasible cause, particularly applicable to the external bootable drives and disabling of the password protecting the boot order. System administrators are responsible for maintaining the functionality of laptop computers. On occasion, they may need to change settings to access the laptop's hard drive using an external drive, particularly if the hard drive is not working correctly. It is possible that the system administrator may forget to change the setting back to its original state when he or she has completed the task.

Due to the nature of the problems we identified, we conclude that these conditions resulted because local system administrators did not follow IRS guidelines in some cases and, during the configuration process, the Information Technology Services did not follow prescribed procedures.

Recommendations

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

1. Remind telecommuting employees periodically to store and encrypt sensitive information on secure locations of their laptop computers.
2. Remind system administrators to reset security settings after servicing laptop computers.

Management's Response: The Director, Mission Assurance, will send out periodic reminders to employees and system administrators on protecting sensitive data on laptop computers and on resetting security settings after servicing laptop computers, respectively. The Director, End User Equipment and Services, will provide the messages for those communication reminders.

3. Develop guidance to assist functional managers in determining whether sensitive data are being stored in unencrypted areas on their employees' laptop computers.

Management's Response: Because this recommendation aligns with Recommendation 6, management's response and our comments will be presented below.

4. Require that the encryption key for VPN laptop computers be stored on external media such as disks or smart cards separate from the computers' hard drives.

Management's Response: The Acting Deputy Commissioner for Modernization & CIO did not concur with this recommendation. While he agreed that the encryption key must be adequately protected, there are no absolute Department of the Treasury or IRS requirements for a hardware token solution for remote access (i.e., external media encryption keys). In addition, the VPN software solution has gone through a full security certification, and the managed services for the VPN solution provide a number of risk mitigation mechanisms.

Office of Audit Comment: Even though management has decided to accept the risk of not maintaining the encryption key separate from the hard drive, we still believe it is prudent to maintain them separately.

5. Consider purchasing commercial software to provide FIPS-compliant encryption scheme software for laptops used in telecommuting.

Management's Response: The Director, End User Equipment and Services, will research FIPS-compliant replacement technology for the current file encryption solutions and will recommend the best course of action for implementation to the Acting Deputy Commissioner for Modernization & CIO.

The Commissioners of the Large and Mid-Size Business, Small Business/Self-Employed, and Tax Exempt and Government Entities Divisions, and the Chief, Agency-Wide Shared Services, should:

6. Require front-line managers to periodically check their employees' laptop computers to ensure that sensitive data are being stored and encrypted properly.

Management's Response: IRS management partially concurred with Recommendations 3 and 6. While they agree that employees should comply with encryption steps for safeguarding data on laptop computers, they believe IRS security professionals, rather than front-line managers, should conduct compliance reviews to ensure encryption policies are being followed. To ensure enterprise-wide consistency for reviewing this issue, they will develop sampling criteria, develop review methodology, and conduct follow-up actions from review results.

Office of Audit Comment: We do not believe that merely asking the security professionals to review a sample of laptop computers will correct the issue. While we recognize the many demands on front-line managers, periodically reviewing employees' laptop computers to ensure proper encryption should be considered an integral responsibility for managers and should not be difficult or time-consuming.

Secure Infrastructures Were Provided for Employees to Connect to the Network, but Improvements Can Be Made

The computer infrastructures supporting both the SDI and VPN connections provided secure means for employees to connect to the IRS network. All transmissions, when properly done, were encrypted. Our attempts to hack into the IRS architecture through the dial-up connections were unsuccessful. However, improvements in the following areas are needed to enhance the security of both architectures.

The firewall systems protecting the VPN main servers were not consistently configured and were not kept current

The VPN architecture consists of two sites, with each site maintaining two internal and two external firewalls. The configurations between the sites and even within the same site were not consistent. Inconsistencies in the setup of the firewalls increase the complexity of the firewall systems and therefore increase the difficulty in maintaining, monitoring, and administrating those firewalls. As a result, attacks against the systems may not be timely identified, and the systems may even fail.

The IRS' Computer Security Incident Response Center (CSIRC) is responsible for monitoring and maintaining the firewalls. The CSIRC had not routinely reviewed the firewall configurations for consistency.

In addition, the firewalls had not been kept current as vulnerabilities were identified by the computer industry. Over 9 months had elapsed since the internal firewalls had been patched. The operating system vendor had issued 51 recommended security patches during this time. The vendor of the external firewalls stopped supporting the installed version at least 8 months before our review began. Upgrading software and installing patches is one of the simplest and most effective ways for reducing risks to computer systems.

Prompt action is important to minimize the time available to potential intruders between detection of a problem and installation of the updated software or corrective patch. The outbreaks of the Code Red and NIMDA worms demonstrated why patching applications and operating systems is critical. The Code Red worm infected more than 300,000 computers in 1 week, even though the patch had been available for several weeks. The NIMDA worm infected a large number of additional computers. The

CERT® Coordination Center[11] estimated that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches.[12] The CSIRC had not devoted sufficient attention to upgrading software and installing patches for the firewalls.

Personal firewall and intrusion detection system (IDS) software was not installed on all laptop computers

Personal firewall and IDS software provides users who connect to the Internet with protection against hackers. It can stop malicious traffic and send alerts about ongoing attacks for immediate action by incident response personnel. The IRS recognized the risks of VPN connections through the Internet and installed this type of software on VPN laptop computers. The IRS' CSIRC centrally monitored network traffic logs generated from the software on VPN laptop computers and further investigated suspicious activities. However, for SDI laptop computers, this type of software was not installed.

Personal firewall and IDS software was not installed on SDI laptop computers because these laptops are designed to connect to the IRS network through telephone lines, which is generally a lower-risk environment than access via the Internet. However, it is possible that an employee could connect the laptop computer directly to the Internet, for example in a hotel room or via his or her home high-speed Internet connection. Once a computer is connected to the Internet, there is no protection for that computer against being attacked. We recognize that this behavior is against IRS policy, but there is no mechanism to prevent it.

[11] The CERT® Coordination Center is a center of Internet security expertise, located at the Software Engineering Institute, a Federally funded research and development center operated by Carnegie Mellon University.

[12] NIST Special Publication 800-40: *Procedures for Handling Security Patches*.

Recommendations

The Acting Deputy Commissioner for Modernization & CIO should:

7. Standardize VPN firewall configurations and hold the CSIRC responsible for maintaining those configurations and installing patches timely.

Management's Response: The Director, Mission Assurance, will continue to use the CSIRC's Firewall Install Guide for deployment of firewall configurations and will take actions to timely install patches to firewall software.

8. Consider installing personal firewall and IDS software on SDI laptop computers and require the CSIRC to centrally monitor the generated logs.

Management's Response: The Director, Enterprise Networks, will replace all remote access capabilities with a project that is currently being developed, the Enterprise Remote Access Project (ERAP). With the implementation of the ERAP, the Director, End User Equipment and Services, will build and deploy an enterprise class personal firewall and IDS to all computers that access the IRS network remotely.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate actions taken by the Internal Revenue Service (IRS) to reduce the risks associated with telecommuting. We defined telecommuters as those employees allowed to work away from the office, either on-site with taxpayers, at home, or at Federal Government telecommuting sites. We focused the review on the security of data on laptop computers used by employees allowed to work away from the office and the security of network connectivity of these employees when they are away from the office. These employees used the two main methods of connecting to the IRS network from the outside: Secure Dial-In (SDI) and the Large and Mid-Size Business Division's Virtual Private Network (VPN) pilot. To accomplish our overall objective, we evaluated:

I. The adequacy of security policies and procedures that have been established to guide telecommuters and the Mobile Workplace program.

II. The effectiveness of security policies and procedures implemented for employees supported by the SDI architecture. We judgmentally selected and reviewed a sample of 86 of over 30,000 SDI laptop computers from the Information Technology Services and Agency-Wide Shared Services organizations, and the Large and Mid-Sized Business, Small Business/Self-Employed, and Tax Exempt and Government Entities Divisions in the IRS' offices in Baltimore, Chicago, and Detroit. We also reviewed the computer architecture allowing SDI employees to connect to internal networks from outside of the office and the protection of SDI resources at the Martinsburg Computing Center.[1]

III. The effectiveness of security policies and procedures implemented for the Large and Mid-Size Business Division's VPN pilot. We judgmentally selected and reviewed a sample of 19 of over 2,000 VPN laptop computers at taxpayers' sites located in Detroit and Chicago. We also reviewed the VPN architecture for allowing employees to connect to the internal networks from taxpayers' sites and evaluated the protection of VPN resources at the Detroit Computing Center.

IV. The effectiveness of security policies and procedures implemented for physical security, incident reporting, and response to laptop computers lost by or stolen from SDI and VPN employees.

[1] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Bill Lessa, Senior Auditor
Midori Ohno, Senior Auditor
Tom Nacinovich, Senior Auditor
Larry Reimer, Senior Auditor
Charles Ekholm, Auditor
Suzanne Noland, Auditor
William Simmons, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Chief Financial Officer, Department of the Treasury
Deputy Commissioner for Operations Support N:DC
Deputy Commissioner for Services and Enforcement N:DC
Commissioner, Large and Mid-Size Business Division LM
Commissioner, Small Business/Self-Employed Division S
Commissioner, Tax Exempt and Government Entities Division T
Chief, Information Technology Services M:I
Chief, Security Services M:S
Chief, Agency-Wide Shared Services A
Director, End User Equipment and Services M:I:EU
Director, Enterprise Operations M:I:EO
Director, Portfolio Management M:R:PM
Audit Liaisons:
Acting Deputy Commissioner for Modernization & Chief Information Officer M
Commissioner, Large and Mid-Size Business Division LM

Appendix IV

Management's Response to the Draft Report

DEPUTY COMMISSIONER

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

RECEIVED
JUN 11 2003

JUN 10 2003

MEMORANDUM FOR ACTING TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: David A. Mader
Acting Deputy Commissioner for Modernization and Chief Information Officer

SUBJECT: Response to Draft Audit Report – Actions Taken to Reduce the Risks of Telecommuting Were Not Adequate (Audit #200220031)

I have reviewed your report evaluating our actions to reduce risks associated with telecommuting. While telecommuting provides benefits for both the Federal Government and its employees, it poses certain security risks. I assure you that safeguarding taxpayer information is one of our agency's highest priorities, and we have taken, and we will continue to take aggressive action to strengthen security controls to mitigate these security risks. As you acknowledged in this report, our accomplishments include:

- Establishing adequate security policies and procedures on laptop security for employees working away from the IRS
- Providing a secure means for employees to connect to the IRS network

We partially concur with the general intent of recommendations three and six in that we believe laptops should be periodically checked for sensitive information being properly stored and encrypted. However, we do not believe that the front-line manager should conduct that review. Instead we will have security professionals conduct the review then report the results to and recommend follow-up actions to the functional manager.

We do not concur with recommendation four requiring that the encryption key for Virtual Private Network (VPN) laptop computers be stored on external media separate from the computers' hard drives. While the encryption key data must be adequately protected, neither Treasury nor IRS security policy has an absolute requirement for a hardware token solution for remote access, except from International locations. However, we do employ a VPN software solution that is a Federal Information Processing Standard compliant product that was

implemented under a full security certification. For more details, see the attached response that addresses each of your report recommendations.

If you have any questions, please call me at (202) 622-6800 or Mary R. Hernandez, Director, Security Policy Support and Oversight at (202) 283-4500.

Attachment

Management response to Draft Audit Report –Security Over Computers Used In Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 1: The Deputy Commissioner for Modernization & Chief Information Officer should remind telecommuting employees periodically to store and encrypt sensitive information on secure locations of their laptop computers.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The Director, Mission Assurance will plan and periodically deliver communications reminders to employees throughout the year on protecting sensitive data which includes storing and encrypting information on their laptop computers. The Director, End User Equipment and Services will provide the content of the communications reminders.

IMPLEMENTATION DATE:

September 30, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)
Responsible Partner:
Director, End User Equipment and Services (M:I:EU)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used In Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 2: The Deputy Commissioner for Modernization & Chief Information Officer should remind system administrators to reset security settings after servicing laptop computers.

CORRECTIVE ACTION TO RECOMMENDATION #2:

The Director, Mission Assurance will plan and periodically deliver communications reminders to system administrators to reset security settings after servicing laptop computers. The Director, End User Equipment and Services will provide the content of the communications reminders.

IMPLEMENTATION DATE:

September 30, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)
Responsible Partner:
Director, End User Equipment and Services (M:I:EU)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used In Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 3: The Deputy Commissioner for Modernization & Chief Information Officer should develop guidance to assist functional managers in determining whether sensitive data are being stored in unencrypted areas on their employees' laptop computers.

CORRECTIVE ACTION TO RECOMMENDATION #3:

We partially concur with the recommendation. We agree that employees' compliance with encryption steps for safeguarding data on laptops is important. However, the IRS believes that in order to ensure enterprise-wide consistency, the review of laptops should be conducted by IRS security professionals. In this regard, please refer to the corrective actions for recommendation #6.

IMPLEMENTATION DATE:

January 15, 2004

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight (M:S:S)
Responsible Partner:
Director, End-User Equipment and Services (M:I:EU)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used In Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 4: The Deputy Commissioner for Modernization & Chief Information Officer should require that the encryption key for Virtual Private Network (VPN) laptop computers' be stored on external media such as disks or smart cards separate from the computers' hard drives.

CORRECTIVE ACTION TO RECOMMENDATION #4:

We do not concur with this recommendation. While the encryption key data must be adequately protected, neither Treasury nor IRS security policy has an absolute requirement for a hardware token solution for remote access, except from International locations. The current Large and Mid-Size Business (LMSB) VPN software solution is a Federal Information Processing Standard (FIPS) compliant product offering that has been implemented under a full security certification. A number of the risk mitigation mechanisms are provided by the 24X7 managed services provisions under this contract that allow the VPN account and sessions to be deactivated remotely if an employee reports the laptop stolen.

Additionally, the LMSB VPN client software stores the private key, encrypted, on the hard drive in a specially designed and created secure E2Rom file. This private key is used with the public key during authentication. At the time of authentication this key is computed with specific PC information, including the hard drive serial number. The VPN client, and its respective private key, can thus only be used from the specific machine for which it was configured. Copies installed on other systems will not be recognized and sessions initiated from other machines will not be established. It is also important to note that the private key is used only for authentication. It is not used to encrypt the information being transmitted. This is done on a per session basis and is generated randomly by the managed service provider. Finally, the private key is not used to encrypt the information for storage on the hard drive. File encryption mechanisms will provide this protection. (See our response to Recommendation 5). We will continue to work with the developer of the VPN client software to take advantage of additional security enhancements as they are developed.

IMPLEMENTATION DATE:

None

RESPONSIBLE OFFICIAL:

None

CORRECTIVE ACTION MONITORING PLAN:

None

Management response to Draft Audit Report –Security Over Computers Used in Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 5: The Deputy Commissioner for Modernization & Chief Information Officer should consider purchasing commercial software to provide FIPS-compliant encryption scheme software for laptops used in telecommuting.

CORRECTIVE ACTION TO RECOMMENDATION #5:

The Director, End User Equipment and Services, is investigating technology to replace the current file encryption solution. Once implemented, the technologies under consideration will provide 3DES (minimum) or AES data encryption protection for IRS information stored on laptops. At conclusion of the current investigative activity, the Director, End User Equipment and Services, will recommend a best course of action for implementation to the Chief Information Officer.

IMPLEMENTATION DATE:

For Enterprise Data Encryption Decision:
December 15, 2003

RESPONSIBLE OFFICIAL:

Director, End-User Equipment and Services (M:I:EU)
Responsible Partners:
Director, Enterprise Networks (M:I:EN)
Director, Mission Assurance (M:S:A)
Director, Security Policy Support and Oversight (M:S:S)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used In Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 6: The Commissioners of Large and Mid-Size Business Division, Small Business/ Self-Employed Division, and Tax Exempt & Government Entities Division, and the Chief, Agency-Wide Shared Services should require front-line managers to periodically check their employees' laptop computers to ensure that sensitive data are being stored and encrypted properly

CORRECTIVE ACTION TO RECOMMENDATION #6:

We partially concur with the recommendation. We agree that employees' compliance with encryption steps for safeguarding data on laptops is important. However, the IRS believes that in order to ensure enterprise-wide consistency, the review of laptops should be conducted by IRS security professionals rather than front-line managers. In this regard, IRS will:

- Develop criteria for determining sample size,
- Develop review methodology, and
- Conduct follow-up actions based on review results.

IMPLEMENTATION DATE:

January 15, 2004

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight (M:S:S)
Responsible Partner:
Director, End-User Equipment and Services (M:I:EU)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used in Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 7: The Deputy Commissioner for Modernization & Chief Information Officer should standardize Virtual Private Network (VPN) firewall configurations and hold the CSIRC responsible for maintaining those configurations and installing patches timely.

CORRECTIVE ACTION TO RECOMMENDATION #7:

The Computer Security Incident Response Center (CSIRC) has published and routinely uses the Firewall Install Guide for the routine deployment of IRS Firewalls. The presence of user accounts not conforming to the IRS naming conventions on the firewall does not by itself diminish the existence nor effectiveness of the Guide.

Actions are being taken to apply timely patches to the underlying operating system of the IRS Enterprise Firewalls. Also, IRS has provided and will continue to provide timely patches to the actual firewall software which poses a much more immediate threat. To mitigate the adverse effects on the supported applications, CSIRC conscientiously works with the firewall vendor to ensure that the Solaris patches will not disrupt critical IRS business processes supported by these devices. In providing timely patches, CSIRC balances the fact that portions of the IRS networking infrastructure and its supporting components are 'stationary' during peak filing season to facilitate the uninterrupted flow of taxpayer data.

IMPLEMENTATION DATE:

August 3, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.

Management response to Draft Audit Report –Security Over Computers Used in Telecommuting Needs to Be Strengthened (Audit #200220031)

RECOMMENDATION # 8: The Deputy Commissioner for Modernization & Chief Information Officer should consider installing personal firewall and IDS software on SDI laptop computers and require CSIRC to centrally monitor the generated logs.

CORRECTIVE ACTION TO RECOMMENDATION #8:

a) The Director, Enterprise Networks will replace all remote access capabilities including SDI through the deployment activities of a project that is currently being developed, Enterprise Remote Access Project (ERAP). It is in alignment with TIGTA recommendations.

There is no other ready solution and SDI cannot be modified as recommended. ERAP is in the evaluation stage, and once evaluation is completed, it will be tested in a lab to ensure that all IRS requirements can be met. The ERAP solution will then be submitted for security certification. Implementation of the new systems is expected to begin the second half of calendar year 2004 and be completed the second half of calendar year 2006. The implementation date was established based on the projected availability of funds and the extent of implementation that includes SDI (over 27,000 users) and other remote users.

b) With the implementation of the Enterprise Remote Access Project, the Director, End User Equipment and Services (EUES) will build an enterprise class Personal Firewall and Intrusion Detection System (PFI). Subsequently, EUES will deploy PFI client software to all computers that access the IRS network remotely and operate the PFI systems infrastructure components.

c) The vendor that is chosen for the Enterprise Remote Access Project (ERAP) will be required to conduct routine "level one" log analysis as outlined by the Computer Security Incident Response Center (CSIRC), under the Director of Mission Assurance; and to report incidents that meet this criteria to the CSIRC Operations Center. CSIRC will be responsible for forensics and investigating identified incidents as reported by the ERAP vendor based on the IRS CSIRC and Treasury Incident Categories.

IMPLEMENTATION DATE(S):

a) December 15, 2006

Milestones –	Complete Evaluation Phase	8/01/03
	Complete Testing	09/01/03
	Obtain Security Certification	03/01/04
	Initiate Implementation Phase	07/01/04
	Complete Implementation Phase	12/15/06

b) December 15, 2006

c) December 15, 2006

RESPONSIBLE OFFICIAL(S):

a) Director, Enterprise Networks (M:I:EN)

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

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

CORRECTIVE ACTION MONITORING PLAN:

Progress towards completing this corrective action will be tracked through regular program oversight activities.