



*The Internal Revenue Service Is Not
Adequately Protecting Taxpayer Data on
Laptop Computers and Other Portable
Electronic Media Devices*

March 23, 2007

Reference Number: 2007-20-048

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.

Redaction Legend:

3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals

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 23, 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 – The Internal Revenue Service Is Not Adequately
Protecting Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices (Audit # 200620001)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) is adequately protecting sensitive data on laptop computers and portable electronic media devices. The audit focused on the security of laptop computers and the encryption of sensitive data maintained on laptop computers. We also evaluated the storage methods for backup tapes at non-IRS offsite facilities.

Impact on the Taxpayer

The IRS annually processes more than 220 million tax returns containing personal financial information and personally identifiable information such as Social Security Numbers. We found hundreds of IRS laptop computers and other computer devices had been lost or stolen, employees were not properly encrypting data on the computer devices, and password controls over laptop computers were not adequate. As a result, it is likely that sensitive data for a significant number of taxpayers have been unnecessarily exposed to potential identity theft and/or other fraudulent schemes.

Synopsis

IRS employees reported the loss or theft of at least 490 computers between January 2, 2003, and June 13, 2006. No organization is impervious to theft or loss of computers, especially an organization as large as the IRS with approximately 100,000 employees. Many incidents cannot be prevented, but employees can reduce the risk by taking precautions. For example, because a



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

large number of laptop computers were stolen from vehicles and employees' residences, employees may not have secured their laptop computers in the trunks of their vehicles or locked their laptop computers at home. Further, because 111 incidents occurred within IRS facilities, employees were likely not storing their laptop computers in lockable cabinets while the employees were away from the office.

IRS procedures require employees to report lost or stolen computers to the IRS Computer Security Incident Response Center (CSIRC) and to the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations. Employees reported the loss or theft of at least 490 computers and other sensitive data in 387 separate incidents. Employees reported 296 (76 percent) of the incidents to the TIGTA Office of Investigations but not to the CSIRC. In addition, employees reported 91 of the incidents to the CSIRC; however, 49 of these were not reported to the TIGTA Office of Investigations. Coordination was inadequate between the CSIRC and the TIGTA Office of Investigations to identify the full scope of the losses.

We found limited definitive information on the lost or stolen computers, such as the number of taxpayers affected, when we conducted our review. However, we conducted a separate test on 100 laptop computers currently in use by employees and determined 44 laptop computers contained unencrypted sensitive data, including taxpayer data and employee personnel data. As a result, we believe it is very likely a large number of the lost or stolen IRS computers contained similar unencrypted data. Employees did not follow encryption procedures because they were either unaware of security requirements, did so for their own convenience, or did not know their own personal data were considered sensitive. We also found other computer devices, such as flash drives, CDs, and DVDs, on which sensitive data were not always encrypted. We reported similar findings in July 2003, but the IRS had not taken adequate corrective actions.

In addition to encryption solutions to protect sensitive data on its laptop computers, the IRS requires controls, such as usernames and passwords, to restrict access to laptop computers. However, 15 of the 44 laptop computers with unencrypted sensitive data had security weaknesses that could be exploited to bypass these security controls. We believe system administrators either incorrectly configured the computers upon deployment or did not correctly reset the controls after working on the computers.

We also evaluated the security of backup data stored at four offsite facilities. Backup data were not encrypted and adequately protected at the four sites. For example, at one site, non-IRS employees had full access to the storage area and the IRS backup media. Envelopes and boxes with backup media were open and not resealed. At another site, one employee who retired in March 2006 had full access rights to the non-IRS offsite facility when we visited in July 2006. Also, inventory controls for backup media were inadequate. We attributed these weaknesses to a lack of emphasis by management.



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

Recommendations

We recommended the Chief, Mission Assurance and Security Services, refine incident response procedures to ensure sufficient details are gathered regarding taxpayers potentially affected by a loss; coordinate with business units to better quantify past incidents; periodically remind employees of their responsibilities for protecting computer devices; consider purchasing computer cable locks for employees' laptop computers; and periodically publicize an explanation of employees' responsibilities for preventing the loss of computer equipment and taxpayer data, the penalties for negligence over these responsibilities, and a summary of actual violation statistics and disciplinary actions.

We recommended the Chief Information Officer include a reminder about encrypting sensitive information in the employees' annual certification of security awareness, including instructions on using approved encryption software on electronic media devices, such as flash drives; require front-line managers to periodically check their employees' laptop computers to ensure encryption solutions are being used by employees; consider implementing a systemic disk encryption solution on laptop computers that does not rely on employees' discretion as to what data to encrypt; require system administrators to check security configurations when servicing computers; implement procedures to encrypt backup data sent to non-IRS offsite facilities; and ensure employees assigned to oversee these facilities conduct an annual inventory validation of backup media and a physical security check of the offsite facility used to store the media.

Response

IRS management agreed with all of our findings and most of the recommendations. For Recommendations 5 and 7, the IRS offered alternative corrective actions that adequately addressed our findings. We concur with the planned corrective action for Recommendation 5 and encourage the IRS to consider publishing annual statistics on disciplinary penalties. We also concur with the alternative corrective action for Recommendation 7 because implementation of disk encryption no longer requires employee actions to encrypt sensitive data. Management's complete response to the draft report is included as Appendix VI.

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.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Table of Contents

Background	Page 1
Results of Review	Page 4
Employees Reported the Loss or Theft of at Least 490 Computers and Other Sensitive Data in 387 Incidents From January 2003 to June 2006	Page 4
<u>Recommendations 1 and 2:</u>	Page 6
Physical Security Was Not Adequate Over Computer Equipment.....	Page 7
<u>Recommendations 3 through 5:</u>	Page 10
Sensitive Data Were Not Encrypted on Laptop Computers and Other Electronic Media.....	Page 11
<u>Recommendations 6 through 8:</u>	Page 14
Access Controls on Laptop Computers Could Be Easily Circumvented.....	Page 15
<u>Recommendation 9:</u>	Page 17
Backup Data Were Not Encrypted and Adequately Protected	Page 17
<u>Recommendations 10 and 11:</u>	Page 19
Appendices	
Appendix I – Detailed Objectives, Scope, and Methodology.....	Page 21
Appendix II – Major Contributors to This Report	Page 24
Appendix III – Report Distribution List	Page 25
Appendix IV – Outcome Measure	Page 26
Appendix V – Office of Management and Budget Memoranda.....	Page 27
Appendix VI – Management’s Response to the Draft Report	Page 28



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Background

The Internal Revenue Service (IRS) annually processes more than 220 million tax returns containing personal financial information and personally identifiable information such as Social Security Numbers. If lost or stolen, taxpayer data can be used for identity theft and/or other fraudulent purposes. Identity theft refers to a crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for financial or economic gain. According to the Federal Bureau of Investigation, identity theft is one of the fastest growing white collar crimes in the United States. The Department of Commerce estimates that more than 50 million identities were compromised in 2005.

Recently, safeguarding personally identifiable information has received much publicity. For example:

- In September 2006, the Department of Commerce reported 1,138 lost, stolen, or missing laptop computers since 2001. Of these laptop computers, 249 contained sensitive information that identified individuals.
- In May 2006, the Department of Veterans Affairs reported a stolen external hard drive. According to an audit performed by the Department of Veterans Affairs Office of Inspector General, the drive contained personal information on approximately 26 million veterans and United States military personnel. The data stolen were primarily limited to individuals' names, dates of birth, and Social Security Numbers.
- In April 2006, a data storage company announced losing a container of backup tapes that included personal information belonging to as many as 17,000 current and former employees of the Long Island Railroad. The IRS uses the same storage company to store backup data for some Area Offices.¹
- Also in April 2006, the news media reported that flash drives² previously owned by the Department of Defense were stolen from a military base and sold in an open market in a foreign country. The flash drives contained potentially sensitive military intelligence data, including the names, photographs, and telephone numbers of spies/informants working for the United States military. According to the news media, the documents appeared to be authentic, but the accuracy of the information could not be independently verified.

¹ Area Offices are located throughout the United States; they serve as the coordination point for and assist the public with tax issues.

² A flash drive is an external data storage device that plugs into the computer and emulates a small disk drive. It allows data to be easily transferred from one computer to another.



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

Most IRS employees use taxpayer information to carry out their responsibilities within the protection of IRS facilities; however, some employees are allowed to take electronic taxpayer data outside of the office for business purposes. For example, revenue agents may take electronic taxpayer records with them when conducting onsite visits to business taxpayers. In addition, as of July 2006, more than 25,000 IRS employees had the ability to access the IRS network from outside of IRS facilities. Overall, the IRS has over 47,000 portable laptop computers assigned to its employees.

Because taxpayer data are allowed to be taken outside of IRS facilities, additional security controls are required, such as:

- Physically protecting computer devices – Employees in possession of computer devices must adhere to specific security policies and handling procedures to minimize the chance of loss or theft of the device. For example, when transporting a laptop computer in a vehicle, an employee should store the computer in the vehicle’s trunk or a place that is not visible from outside of the vehicle.
- Encrypting³ taxpayer data on computer devices – Even if a computer device is lost or stolen, the data can be protected if the data are encrypted. Encryption ensures no one other than the authorized user can access and view the data maintained on the computer device.
- Using software controls to limit access to computers – If a computer is lost or stolen, the data can still be protected to some degree by requiring the user to enter a valid username and corresponding password soon after starting up the computer. This control can sometimes be bypassed if the computer is not properly configured.
- Reporting incidents – Any employee who loses a computer must follow specific reporting instructions to ensure the proper authorities are notified. Actions should then be taken to disable user accounts and to look for clues, in case an attempt is made to use the computer to access the IRS network.

In addition, data that are backed up and stored offsite so operations can be restored in the event of a disaster may also be at risk.⁴ If the backup location is not within the organization’s control (e.g., a contractor’s site), security policies and procedures must be implemented to ensure the data are protected from unauthorized access and fully accounted for.

³ Encryption is a method to convert readable text (i.e., plaintext) to unreadable text (i.e., ciphertext) by applying mathematical algorithms and one or more encryption keys. This is generally performed to protect the confidentiality, integrity, and authenticity of data during storage or transmission.

⁴ In the event of a disaster, it is possible that all data maintained at a facility where the disaster occurred could be destroyed. For example, a building fire might destroy all data stored at the facility. An organization can reduce this risk by maintaining backup data at a different facility.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

This review was part of our Fiscal Year 2006 Annual Audit Plan and was based on our findings from previous years of noncompliance in safeguarding taxpayers' data.⁵ We recognized the enormous risk of having taxpayer data outside of IRS offices and the importance of establishing policies and procedures, implementing security solutions to protect taxpayer data, educating employees on protecting taxpayer data, and following up to ensure security solutions are working as intended. As such, we had initiated this review prior to the Department of Veterans Affairs theft incident. During our review, the Office of Management and Budget⁶ issued several memoranda to Federal Government agencies on the topic of safeguarding personally identifiable information. Appendix V provides a brief explanation of these Office of Management and Budget memoranda.

This review was performed at the Area Offices in New Carrollton, Maryland; Laguna Niguel, California; Atlanta, Georgia; Cincinnati, Ohio; and Salt Lake City, Utah; the Campuses⁷ in Fresno, California; Atlanta, Georgia; Covington, Kentucky; and Ogden, Utah; and 4 non-IRS offsite facilities located fewer than 40 miles from the 4 Area Offices (excluding the Area Office in New Carrollton, Maryland) during the period April through December 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.

⁵ *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006) and *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (Reference Number 2003-20-118, dated July 2003).

⁶ The Office of Management and Budget ensures Federal Government agencies' reports, rules, testimony, and proposed legislation are consistent with the President's budget and with administration policies. The Office of Management and Budget's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public.

⁷ 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.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Results of Review

Employees Reported the Loss or Theft of at Least 490 Computers and Other Sensitive Data in 387 Incidents From January 2003 to June 2006

On June 15, 2006, we requested that the IRS provide us information on all incidents relating to the loss or theft of computer devices since April 2005. To fulfill our request, the IRS researched its own records from the IRS Computer Security Incident Response Center (CSIRC)⁸ and validated its information with the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations, the law enforcement organization for internal IRS affairs. On July 10, 2006, the Chairman of the House Committee on Government Reform sent a letter to the Secretary, Department of the Treasury, requesting information on all incidents since January 1, 2003, involving the loss or compromise of any sensitive personal information held by the Department of the Treasury. As a result of our request and the House Committee on Government Reform letter, the IRS compiled a list of 387 incidents, including the loss or theft of at least 490 computers⁹ from January 2, 2003, to June 13, 2006.

IRS procedures require that, when computers are lost or stolen, employees must report the incident to the TIGTA Office of Investigations for further investigation and possible recovery efforts. In addition, employees must report the incident to the CSIRC for tracking actions, such as determining if anyone has attempted to use the computers to access the IRS network and follow-on actions such as canceling remote access accounts.

Prior to our June 2006 request for information on all incidents relating to the loss or theft of computer devices and/or personally identifiable information, the CSIRC was made aware of only 91 (24 percent) of the 387 incidents. Of the 91 incidents reported to the CSIRC, 42 were also reported to the TIGTA Office of Investigations and 49 were not. The

Employees did not properly report 76 percent of all incidents of lost or stolen computers and/or sensitive data to the IRS CSIRC.

⁸ The CSIRC provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.

⁹ The 387 incidents included those for which the IRS was unable to determine the exact number of stolen or lost computers because that information was not captured in its database of incidents. Consequently, the number of lost or stolen computers for these incidents was counted as "1+." On November 15, 2006, radio station WTOG reported 478 IRS laptop computers were lost or stolen between 2002 and 2006. The radio station had obtained the information from the IRS through the Freedom of Information Act (5 U.S.C.A Section 552 (West Supp. 2003)). We attribute the difference in our results to the nature of information that can be released under the Freedom of Information Act and to different time periods covered by our audit and the station WTOG request.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

TIGTA Office of Investigations was aware of 296 (76 percent) of the 387 incidents, none of which had been reported to the CSIRC.

When computer equipment is lost or stolen, the primary concern is the data contained on the computer. In conjunction with the CSIRC, we evaluated all 387 incidents to determine how many involved the loss or compromise of personally identifiable information and to identify the impact to taxpayers.

We were unable to determine the full impact to the taxpayers for many of the incidents involving the loss or theft of computer equipment and/or taxpayer data.

We determined it was unlikely that 176 (45 percent) of the 387 incidents involved taxpayer data. For the remaining 211 incidents, we analyzed the incident writeups as of June 2006 and found 126 contained sufficient details to show that personal information for at least 2,359 individuals was involved with the incidents. We were unable to identify the nature of the data loss and the identities of taxpayers whose information may have been lost for the other 85 of 211 incidents due to lack of details in the incident writeups.

We believe IRS employees who reported incidents to the TIGTA Office of Investigations did not extend the reporting process to their own internal computer security organization. We surmised that employees were mainly concerned with the reporting of the incidents to law enforcement authorities and the investigation and recovery of the lost or stolen computer equipment. Managers of these employees and information technology support functions, who were involved with replacing computer equipment for the employees, did not ensure the CSIRC was notified of the incidents.

Prior to the Department of Veterans Affairs incident in May 2006, the CSIRC had not placed sufficient emphasis on identifying actual taxpayers potentially affected by lost or stolen computers. The TIGTA Office of Investigations did investigate many of these incidents, but its approach was from a criminal focus (e.g., identifying the perpetrator, recovering the stolen equipment). In addition, coordination between the CSIRC and the TIGTA Office of Investigations was inadequate to identify the full scope of the losses.

On July 7, 2006, the Chief, Mission Assurance and Security Services, issued a memorandum regarding *Updated Guidance for IRS Computer Security Incident Reporting* to all IRS heads of office. This memorandum reemphasized reporting requirements and stated that all computer security incidents shall be reported to the CSIRC and to front-line managers. In addition, any incident involving physical loss of equipment that could result in unauthorized access to IRS systems or information must also be reported to the TIGTA Office of Investigations. Prior to issuance of this memorandum, the IRS Commissioner had issued an email to all IRS managers, reminding them to safeguard personally identifiable information and to immediately report any security incidents to the CSIRC. The email message also stated that, for cyber-security incidents involving access to or disclosure of taxpayer data or possible incidents of identity theft,



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

managers should work with the CSIRC to promptly notify the TIGTA Office of Investigations. As a final measure to ensure total coordination, the IRS is in the process of entering into an agreement with the TIGTA Office of Investigations to share all incidents relating to the loss or theft of information technology assets.

The above corrective actions taken by the IRS during our audit should sufficiently address the causes of the lack of full reporting by employees. However, on July 19, 2006, the Chairman of the House Committee on Government Reform introduced legislation to require Federal Government agencies to make public notifications in the event of data breaches involving sensitive information. The legislation, which would amend the Federal Information Security Management Act,¹⁰ directs the Office of Management and Budget to establish policies, procedures, and standards for agencies to follow if sensitive personal information is lost or stolen. In anticipation of this legislation, we are making the following recommendations.

Recommendations

The Chief, Mission Assurance and Security Services, should:

Recommendation 1: Refine CSIRC reporting and handling procedures to ensure sufficient details are gathered and recorded in the incident writeups regarding taxpayers potentially affected by a loss and the nature of the lost data.

Management's Response: The IRS agreed with this recommendation. The Mission Assurance and Security Services organization has refined the incident handling and reporting procedures to ensure sufficient details are gathered and recorded regarding taxpayers potentially affected by the loss and the nature of the lost data. These refinements include the creation of a Personally Identifiable Information Incidence Working Group, which has developed an incident management policy; a personally identifiable information analysis template; and a risk analysis framework. These efforts have resulted in modification to the CSIRC intake process and a handoff of appropriate incidents to the core response group for disposition.

Recommendation 2: Coordinate with the business units that have reported lost or stolen computer devices since 2003 and quantify the impact to taxpayers in terms of how many taxpayers were affected by the incidents and what personally identifiable information was lost.

Management's Response: The IRS agreed with this recommendation. Between July and September 2006, the Mission Assurance and Security Services organization launched two efforts to refine CSIRC reporting and handling procedures. First, for each of the

¹⁰ This Act is part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301 (2002). The Federal Information Security Management Act includes protecting information and information systems from unauthorized access, use, disclosure, or modification, including controls for disclosure and confidentiality to protect personal privacy.



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

business units that have reported lost or stolen computer devices since 2003, the Mission Assurance and Security Services organization has requested a quantification of the impact to taxpayers and a determination of the lost data. In addition, the CSIRC made modifications to reporting and handling procedures to capture details regarding the types of data elements, the encryption status of each affected asset, and the number of potentially affected individuals.

Second, the Office of Privacy and Information Protection established a cross-functional working group to ensure the appropriate focus on details involving the data and encryption status of each incident. At the same time, the group ensured the reporting and handling of incidents do not violate privacy requirements. The membership of the working group included subject-matter experts from across the IRS (e.g., the Office of Disclosure, the Office of Chief Counsel, the Office of Labor Relations, the CSIRC, and the Office of Privacy and Information Protection).

Physical Security Was Not Adequate Over Computer Equipment

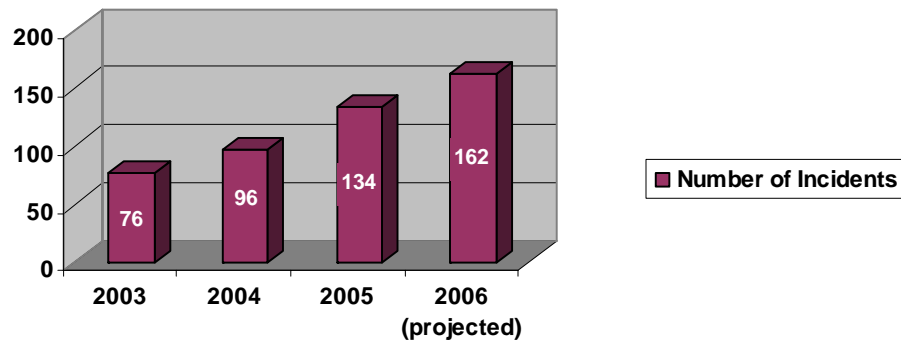
No organization is impervious to theft or loss of computers, especially an organization as large as the IRS with approximately 100,000 employees and over 47,000 laptop computers assigned to its employees. To minimize the risk of theft or loss of computer equipment, the IRS has established basic computer security procedures for its employees. For example, employees are responsible for ensuring security over their laptop computers when not in their possession by storing them in a locked container or physically securing them to immovable furniture with a cable lock when not in use. When in transit, on business trips, or commuting to the workplace, employees shall secure the laptop computer in a vehicle trunk. When traveling by plane, bus, or train, employees shall retain possession of the laptop computer under the seat in front of the employee rather than in an overhead bin. Employees shall not check laptop computers with luggage at airports, leave laptop computers unattended in public places, leave laptop computers in plain view when leaving the hotel room, or leave laptop computers at home where sensitive information can be easily seen.

Despite these security requirements, since 2003 the IRS has been averaging nine incidents per month relating to the theft or loss of computer equipment and/or taxpayer data. Many incidents cannot be prevented; however, because most losses of computer devices and data occur outside of IRS facilities, employees must be particularly cognizant of the risks. The total number of incidents has increased each year, as illustrated in Figure 1.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Figure 1: Number of Incidents of Theft or Loss of Computer Equipment and/or Taxpayer Data (2003 – 2006)



Source: TIGTA analysis and projection based on CSIRC and TIGTA Office of Investigations data.

The projected volume of incidents for 2006 was based on doubling the known volume of 81 incidents from January to June 2006. We believe the recent attention to and current reemphasis on employee responsibility over safeguarding computer equipment and taxpayer data should raise the level of employee awareness, thus reducing the number of preventable incidents. However, understanding the nature and circumstances of the 387 reported incidents may provide insight into how to prevent future losses from occurring. We categorized the 387 incidents by item type, as shown in Figure 2.

Figure 2: Number of Incidents of Theft or Loss of Computer Equipment and/or Taxpayer Data Categorized by Item Type

Item Type	Number of Incidents ¹¹	Actual Number of Items
Laptop Computers	345	477
Desktop Computers	10	13
Peripherals	30	36
ID Badges or Commissions	26	26
Hardcopy Documents	22	171
Tapes or Portable Drives	10	11
Blackberrys or Cell Phones	6	6
Other or Unknown Items	8	69

Source: TIGTA analysis of CSIRC and TIGTA Office of Investigations data.

As Figure 2 illustrates, laptop computers overwhelmingly represent the largest category of lost or stolen items. Because of the portability and monetary value of laptop computers, they tend to be

¹¹ Some incidents involved multiple types of items. Therefore, the number of incidents does not total 387 incidents.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

an attractive target for thieves. The lack of physical security provided to these and other computer devices increased the risk that taxpayer data could be lost or stolen and used for fraudulent purposes. For further perspective, we segregated the incidents by the location where the theft or loss occurred, as presented in Figure 3.

Figure 3: Location of Theft or Loss

Location of Theft/Loss	Number of Incidents	Percentage (Based on 387 incidents)
IRS Facility	111	29%
Vehicle	89	23%
Volunteer Income Tax Assistance Site	53	14%
Residence	35	9%
Hotel	11	3%
Airport	7	2%
Travel Status (specific location not known)	4	1%
Public Transportation (planes, trains, buses)	4	1%
Taxpayer Site	4	1%
Freight Company	4	1%
Unspecified/Unknown Location	65	17%

Source: TIGTA analysis of CSIRC and TIGTA Office of Investigation data.

Figure 3 illustrates areas where the IRS can focus attention when providing additional guidance and assistance to its employees. For example, because 111 incidents occurred within IRS facilities, employees were likely not storing their laptop computers in lockable cabinets while the employees were away from the office. Further, because a large number of laptop computers were stolen from vehicles and employees' residences, employees may not have secured their laptop computers in the trunks of their vehicles or locked their laptop computers at home. Sufficient documentation was not available to evaluate the circumstances surrounding most of the 387 incidents. However, we determined that at least 24 of the incidents could have been prevented if employees had followed IRS policies and procedures.

- Fourteen incidents involved employees storing the laptop computers in unlocked vehicles or in the front seat or back seat of their vehicles, with the computers being visible through the windows, or employees forgetting to place computers into their vehicles.
- Seven incidents involved employees leaving computers on buses and trains and at airports.
- Three incidents occurred because employees checked their computers at an airport.

The 24 incidents involved personally identifiable information for 480 individuals. The loss of these records, which consisted of taxpayer and employee information, also could have been prevented had the incidents not occurred.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

We obtained information on whether disciplinary actions were taken against the responsible employees for 18 of the 24 incidents and found that only 1 employee involved in the 18 incidents was disciplined. The IRS' own guide for penalty determinations indicates the loss of Federal Government property may result in discipline ranging from a written reprimand to a 14-day suspension for a first offense. We believe disciplining employees for security violations resulting from negligence or carelessness could deter others from neglecting their responsibilities for protecting Federal Government property.

Recommendations

The Chief, Mission Assurance and Security Services, should:

Recommendation 3: Provide employees periodic reminders of their responsibilities for protecting computer devices, which, at a minimum, should include storing laptop computers in locking cabinets in the office, storing laptop computers in the trunks of vehicles, and securing laptop computers at home or alternate work locations.

Management's Response: The IRS agreed with this recommendation. It has established a strategic communications team to lead an integrated effort reminding employees of their responsibilities regarding the protection of personally identifiable information and assets, including proper storage of laptop computers.

Between June 2006 and December 2006, the strategic communications team issued several targeted messages to all IRS employees. Employees have also received periodic reminders of their responsibilities for protecting computing devices. In addition, this topic was included on the Information Protection Mandatory Awareness briefing in 2006. This important message will remain a focal point for the strategic communications team and is a standard part of ongoing communications activities.

Recommendation 4: Consider purchasing computer cable locks for employees to provide an additional layer of security at their residence, hotel, or taxpayer site. Instructions should be provided on how to use the locks and the best method to secure the laptop computer to an immobile or heavy object.

Management's Response: The IRS agreed with this recommendation. It purchased combination cable locks for all laptop computers on August 31, 2006, and is distributing the locks to all laptop computer users. In addition, the IRS has established instructions to employees on how to use the lock and issued an interim policy to clarify the use of computer cable locks for employees.

Recommendation 5: Periodically publicize an explanation of employees' responsibilities for preventing the loss of computer equipment and taxpayer data, the associated disciplinary penalties for negligence over these responsibilities, and a statistical summary of actual violations and disciplinary actions relating to loss of computer equipment and taxpayer data.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Management's Response: The IRS agreed with the intent of this recommendation but proposed an alternative corrective action. As a part of the mandatory annual information protection training, the Mission Assurance and Security Services organization will explain employees' responsibilities for preventing the loss of computer equipment and taxpayer data and the associated disciplinary penalties for negligence over these responsibilities. Publicizing statistical summaries presents privacy and labor relations issues for the IRS; therefore, it will implement a communications plan that includes issuing regular announcements highlighting the disciplinary penalties, to remind employees to be vigilant in protecting personally identifiable information and agency equipment.

Office of Audit Comment: We acknowledge that publicizing statistical summaries of actual violations and disciplinary actions relating to loss of computer equipment and taxpayer data could reveal the identity of those employees involved, particularly if the numbers are very low, and possibly violate privacy requirements. Therefore, we concur with the alternative corrective action for this recommendation and encourage the IRS to consider publishing annual statistics on disciplinary penalties, which should hide the identities of employees affected and illustrate the consequences of noncompliance to security policies and procedures.

Sensitive Data Were Not Encrypted on Laptop Computers and Other Electronic Media

On June 8, 2006, the Chief, Mission Assurance and Security Services, testified before the House Committee on Government Reform about the security of taxpayer data on computers used by the IRS. He stated all IRS computers have tools that allow users to encrypt taxpayer data, personally identifiable information, and sensitive information.

The IRS does require all sensitive data on laptop computers to be encrypted. As part of this requirement, the IRS has established two encryption solutions available to employees. First, laptop computers are configured to encrypt data residing in specific file folders on the internal hard drive. This encryption solution is part of the computer's operating system. Employees need only to save sensitive files to these file folders and the computer will automatically encrypt the files. Second, the IRS can provide employees with a separate encryption program to encrypt files. This solution is particularly effective when encrypting files not stored on the computer's internal drive (e.g., files stored on CDs and DVDs).

To test the encryption of sensitive data, we selected 100 laptop computers from 4 IRS Area Offices supporting the Wage and Investment, Small Business/Self Employed, and Large and Mid-Size Business Divisions. We found 44 of the 100 laptop

Sensitive data, such as taxpayer and employee data, were not encrypted on 44 of the 100 laptop computers we reviewed.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

computers contained unencrypted sensitive data. Of these 44 laptop computers, 31 held taxpayer data and 17 held employee personnel data (4 held both taxpayer and personnel data). The following are examples of the unencrypted sensitive data:

- U.S. Individual Income Tax Return (Form 1040).¹²
- U.S. Corporation Income Tax Return (Form 1120).¹³
- Audit-related information, such as case history on current audits and financial data of taxpayers being audited.
- Various IRS forms with Social Security Numbers.
- Employee evaluations, timesheets, and applications for reassignment.

We believe it is very likely a large number of the lost or stolen computers presented in the previous findings contained similar unencrypted data. The IRS had defined directories on the hard drives where sensitive data should have been stored and encrypted. We found, however, that employees frequently placed sensitive data outside of those directories, either because the employees were not aware of the security requirements or for their own convenience. In addition, we found employees did not know that their own personal data were considered sensitive.

In addition to the unencrypted sensitive data on laptop computers, we found other computer devices on which sensitive data were not always encrypted, contrary to IRS procedures. Of the 100 employees in our sample, 20 had small portable flash drives. Fifteen employees informed us that the IRS had purchased flash drives for them, while five employees had purchased their own flash drives although the IRS prohibits the use of privately owned portable electronic devices to process, store, or transmit sensitive IRS information.

- For the 15 employees in possession of IRS-purchased flash drives, we found employees either stored sensitive unencrypted data on the flash drives, used an IRS-approved encryption solution, did not store sensitive data, or did not have the opportunity to use the flash drives.
- For the five employees in possession of self-purchased flash drives, we found employees either stored sensitive unencrypted data, had a system administrator install an encryption program on the flash drive, or did not store sensitive data on the devices.

In addition, 54 of the 100 employees were using various other computer media (e.g., floppy disks, DVDs, and CDs) to store taxpayer data without encryption. For example, employees were

¹² Form 1040 is the IRS form used by individuals to report and file Federal income taxes.

¹³ Form 1120 is the IRS form used by corporations to report and file Federal income taxes.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

using unencrypted CDs to back up taxpayer case information, to store grand jury information, and to retain tax information provided by taxpayers.

During our site visits, various IRS organizations distributed documents regarding the need to encrypt taxpayer data. For example, on June 2, 2006, the Commissioner, Small Business/Self-Employed Division, issued an email to all of his managers and employees reminding them of the IRS security policy for storing files that contain taxpayer information or other sensitive and private information on laptop computers or other portable media storage devices. The email also discussed the process the managers must follow to ensure all employees in their groups understand their responsibilities to protect sensitive data. In addition, several employees informed us they had “cleaned up” the files on their computers prior to our visits. Even with the issuance of this email and the publicity of our review, we did not see improvement from our initial site visit to our last site visit.

Media storage devices, especially flash drives, have become popular and affordable over the last few years. Their small size and portability increase the likelihood that they could be lost or stolen. By not encrypting the data on laptop computers and media devices, the IRS is unnecessarily exposing taxpayer data to unauthorized access, theft, or loss.

In July 2003, we reported¹⁴ that sensitive files were not adequately encrypted on IRS laptop computers. In that report, we made the following recommendations to the IRS that pertained to encrypting sensitive data:

- Periodically remind telecommuting employees to store and encrypt sensitive information in secure locations on their laptop computers.
- Develop guidance to assist functional managers in determining whether sensitive data are being stored in unencrypted areas on their employees’ laptop computers.
- Require front-line managers to periodically check their employees’ laptop computers to ensure sensitive data are being properly stored and encrypted.

The IRS only partially agreed with the third recommendation, stating it agreed that employee compliance with encryption steps for safeguarding data on laptop computers is important. However, the IRS believed that, to ensure enterprise-wide consistency, the review of laptop computers should be conducted by the IRS security professionals rather than front-line managers. To ensure enterprise-wide consistency for reviewing this issue, the IRS agreed to develop sampling criteria, develop review methodology, and conduct followup actions from review results.

In an Office of Audit Comment to management’s response to the July 2003 report, we replied that we did not believe merely asking the security professionals to review a sample of laptop

¹⁴ *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (Reference Number 2003-20-118, dated July 2003).



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

computers would correct the issue. While we recognized 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.

The IRS reported it had completed the corrective action to close the first two recommendations and postponed corrective action on the third recommendation until January 2008. However, we were unable to find any supporting documentation for those closed actions, and it appears the IRS may not have completed the corrective actions as reported. As a result, these issues persist today.

Recommendations

The Chief Information Officer should:

Recommendation 6: Include a reminder in the annual certification of security awareness that employees should store encrypted sensitive information in a secure location on their laptop computers and show them how to use commercial software approved by the IRS to encrypt sensitive data on electronic media devices, such as flash drives.

Management's Response: The IRS agreed with this recommendation. It has developed and implemented a mandatory Information Protection training module and encryption job aides for all employees to remind them of their responsibilities to secure personally identifiable information and how to use available encryption technologies.

Recommendation 7: Require front-line managers to periodically check their employees' laptop computers to ensure encryption solutions are being used by employees and sensitive data are encrypted properly.

Management's Response: The IRS agreed with the intent of this recommendation but proposed an alternative corrective action. The IRS mandated the implementation of disk encryption, which encrypts all contents on the entire hard drive of the computer, for all laptop computers and will issue a policy requiring all employees to annually certify they are using encryption tools properly to protect sensitive data.

Office of Audit Comment: Because the implementation of disk encryption no longer requires employee actions to encrypt sensitive data, we concur with the alternative corrective action to this recommendation.

Recommendation 8: Consider implementing a systemic disk encryption solution on laptop computers. When the entire hard drive is encrypted, employees will no longer have to determine what data need to be encrypted. This solution will supplement the two existing encryption solutions previously discussed.



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

Management's Response: The IRS agreed with this recommendation. It has implemented an enterprise-wide disk encryption initiative and mandated that the systemic disk encryption solution be installed on all laptop computers. This solution encrypts the entire hard drive and requires access authentication whenever a laptop has been turned off. If a laptop computer is lost or stolen, unauthorized users will be unable to access any data on the hard drive.

Access Controls on Laptop Computers Could Be Easily Circumvented

In addition to encryption solutions to protect data on its computer devices, the IRS has implemented security controls (generally referred to as authentication controls¹⁵) to restrict who can access the computers. All laptop computers are equipped with logon screens once the computers are turned on. The user must enter an acceptable username and the associated password before the computer allows the user to access its computing resources.

The password protection mechanism does not activate until the completion of the computer's startup process, which is referred to as the boot process. When a user presses the power button on a computer, the computer automatically initiates the boot process, which causes the computer to execute preset instructions located on the hard drive of the computer including the security processes.

However, a computer's boot process can be interrupted by pressing one of the function keys¹⁶ immediately after powering up the computer. After the boot process is interrupted, the computer may request the user to enter the administrator boot process password. If the boot process password is not enabled, the computer will automatically enter into the boot process settings, where the user can make changes to the boot process like activating or disabling special controls.

For the 44 laptop computers that contained unencrypted sensitive data from the previous finding, we found that 15 computers contained a security weakness in the boot process.

- Three of the 44 laptop computers were configured to boot from a location other than the hard drive. IRS procedures require that all computers boot only from the internal hard drive. When a computer is allowed to boot from the removable media drive (e.g., CD drive), an employee, as well as any hacker, can insert a CD into the computer and the computer will automatically initiate its boot process from that disk. If the CD contains its own operating system, the computer will bypass all security controls established on the computer's operating system, including the password access control.

¹⁵ Authentication controls are used to verify the identity of the user accessing a computer or computer network and generally involve the use of passwords. The computer or computer system would require the input of a valid username and corresponding passwords to proceed with accessing the computer or computer system.

¹⁶ Each computer manufacturer designates a different function key to interrupt the boot process.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

- Six of the 44 laptop computers did not have the password enabled to protect the computers' boot process. IRS procedures require that all computers have this password enabled so only authorized personnel, usually system administrators, can make changes to the boot processes. When no password is enabled to protect the boot order, anyone can interrupt the computer's normal boot sequence, access the boot settings, and change the boot order sequence so the computer will boot from the disk drive as opposed to the computer's hard drive.
- An additional 6 of the 44 laptop computers were configured to boot from a location other than the hard drive and did not have the password enabled to protect the computers' startup process.

We also identified one other significant computer security violation on one of the computers we reviewed. An employee wrote user account names and passwords to the computer and various systems to which the employee has access on a piece of paper that was taped to the laptop computer. The IRS requires employees to safeguard passwords and keep them hidden. If this computer was lost or stolen, the perpetrator would have access to the computer's contents as well as the systems listed on the piece of paper.

Each of these weaknesses could allow unauthorized persons to bypass security controls, including passwords, to gain access to the data on the computers, particularly considering the lack of physical security and encryption controls we previously discussed. We believe system administrators either incorrectly set up the computers upon deployment or did not correctly reset the boot order settings after working on the computers. System administrators are the only individuals who should have knowledge of the boot process password.

We have previously reported findings about weak security settings.¹⁷ In July 2003 and February 2006, we conducted a similar test to determine if laptop computers were properly configured to protect the computers' boot process. The test results revealed that computer startup processes were incorrectly set, similar to what we found in this review. Each report had a recommendation to address this problem.

- In the February 2006 report, we recommended the IRS hold system administrators accountable for ensuring the boot process password is enabled and the boot order lists only the hard drive as the boot initiation process. The IRS responded that there was no way for it to hold system administrators accountable because of the lack of workstation audit trails. However, the Chief Information Officer would issue a memorandum to all

¹⁷ *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006) and *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (Reference Number 2003-20-118, dated July 2003).



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

workstation administrators containing the expectations that the boot process is enabled and that the boot order lists only the hard drive as the boot initiation process.

- In the July 2003 report, we recommended the IRS remind system administrators to reset security settings after servicing laptop computers.

We obtained a memorandum issued on March 20, 2006, by the Chief Information Officer that addressed the February 2006 recommendation. The IRS reported it had completed the corrective actions to close both recommendations. However, we were unable to find any supporting documentation for closing the July 2003 recommendation, even though it was reported as completed. Regardless, actions taken to resolve this issue have not been effective.

Recommendation

The Chief Information Officer should:

Recommendation 9: Require system administrators, when servicing a laptop computer, to check the boot process settings to ensure the boot process password is enabled and the boot order lists only the hard drive as the boot initiation process. System administrators should document completion of this task.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will issue a memorandum that requires all workstation administrators, when servicing a laptop computer, to document the correct boot process settings via an Enterprise Workstation Check List. With the addition of enterprise-wide disk encryption, the boot initiation process is relegated to the hard drive by individuals who possess a disk encryption access profile resident on the workstation.

Backup Data Were Not Encrypted and Adequately Protected

In the event of a disaster such as a fire, it is possible that all data maintained at a facility could be destroyed. The IRS reduces this risk by maintaining backup data at offsite facilities. Because IRS backup data are often sensitive, controls must be in place to protect against unauthorized access, theft, or loss. In addition, the IRS often uses vendors to store backup media, which may increase the risk of unauthorized access.

The National Institute of Standards and Technology recommends that organizations encrypt backup information.¹⁸ At the opening conference for this review, IRS officials informed us the IRS does not encrypt backup media that are sent to offsite facilities. The IRS policy handbook

¹⁸ National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.



***The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices***

covering offsite facilities did acknowledge that the current version of the Commercial Off-the-Shelf backup software does not encrypt data and, therefore, proper protection and handling must be afforded to the backup media.

We validated that the IRS did not encrypt its backup data sent to the four facilities we visited. While we did not identify any significant security weaknesses in how contractors transported backup media from the IRS facilities to their own facilities, we did identify the following physical security and inventory weaknesses:

- At one site, non-IRS personnel at the facility had full access to the storage area and the IRS backup media. The storage area was controlled by a padlock, but the fencing did not extend to the ceiling and could be climbed over to gain access to the storage area. In addition, the IRS requires that magnetic media, which were stored at this site, be packed in heavy-gauge plastic containers provided by the site or the vendor. However, the backup media were stored in simple packing envelopes; staples were used to close the envelopes and tape was used to close the boxes. We observed several opened envelopes and boxes for which no documentation or no notation existed as to who opened them or the date and time they were opened. These envelopes were not resealed. Due to poor inventory controls (discussed below), we were unable to determine if backup data were missing or had been copied.
- At another site, the current list of IRS employees authorized to access the facility and view tapes was not updated. An employee who retired on March 31, 2006, still had full access privileges to the non-IRS offsite facility when we conducted our site visit on July 12, 2006. The employee's name was not timely deleted from the access list.

The annual inventory is the physical verification of the presence of all IRS-owned media. The IRS requires all offices that own, process, ship, receive, or control any type of media to conduct an annual inventory validation, including those media stored at non-IRS premises.

- At one site, we were unable to locate one backup medium from the inventory records and could not confirm what was contained on the medium. In addition, we identified 12 backup media at the storage facility that were not controlled on the inventory lists. These inaccuracies existed because the IRS has not conducted its own reconciliation of the inventory of stored backup media. ^{3(d)}
- At another site, we found seven backup tapes that were not listed on the inventory records. Also, six outdated backup tapes were listed on the inventory list. Additionally, we were unable to reconcile backup disks stored at the non-IRS offsite facility. We identified 289 backup disks, but the inventory list that was provided to us for reconciliation was outdated and several backup disks were recorded more than once on the inventory list. Thus, we could not determine how many backup disks were supposed to be stored at the non-IRS offsite facility. The individual responsible for maintaining the



The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices

inventory list left the IRS in 2004, and a replacement was selected only a month before our site visit. ^{3(d)}

- At a third site, we found one storage container with backup tapes maintained at the site, but the container was not identified on the inventory list.

The lack of encryption on backup data combined with physical security weaknesses and inventory weaknesses increases the risk that sensitive data, including personally identifiable information, could be lost or stolen at backup facilities. We attribute these weaknesses to a lack of emphasis by management.

The National Institute of Standards and Technology recommends data be removed from media, such that there is reasonable assurance the data may not be retrieved and reconstructed. The IRS policy also requires proper disposal of media that contain sensitive data; the IRS has approved degaussing¹⁹ as a method to remove sensitive data from magnetic media. Disposal procedures were adequate at the four sites we visited.

Recommendations

The Chief Information Officer should:

Recommendation 10: Implement procedures to encrypt backup data sent to non-IRS facilities.

Management's Response: The IRS agreed with this recommendation. It will analyze, test, procure, and implement a software-based automated encryption solution to work in conjunction with existing backup technology for servers. In support of mainframe configurations, the IRS will execute a proof of concept test, which includes the use of encryption tape drives along with encryption application technology, to identify the most effective encryption method. Testing will conclude in late Fiscal Year 2007, and formal materials associated with test findings and technical recommendations will be used to develop detailed plans for implementation of encryption in Fiscal Year 2008.

Recommendation 11: Ensure employees who are assigned oversight responsibilities for non-IRS facilities complete the following tasks:

- Conduct and certify an annual inventory validation of backup media.
- Conduct periodic checks to verify the accuracy of the access list and to ensure individuals who no longer have a need to access the non-IRS facilities have been removed.

¹⁹ Degaussing is a process to erase data from a magnetic disk or other storage device.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

- Conduct an annual internal physical security review of the non-IRS offsite facility to determine that the site meets IRS requirements.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will review and update the procedure to ensure oversight responsibilities are clearly defined for the annual inventory validation of backup media, for periodic checks of facilities' access lists, and for annual physical security reviews.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objective of this review was to determine whether the IRS is adequately protecting sensitive data on laptop computers and portable electronic media devices. The audit focused on the security of laptop computers and the encryption¹ of sensitive data maintained on laptop computers. We also evaluated the storage methods for backup tapes at non-IRS offsite facilities. To accomplish our objectives, we:

- I. Evaluated the security policies and procedures established to protect sensitive data on laptop computers and portable electronic storage media, methods of cleansing sensitive data from electronic media, and storage method for backup tapes at non-IRS offsite facilities.
 - A. Evaluated IRS security policies, procedures, and guidelines related to laptop computers and electronic media.
 - B. Evaluated Federal Government guidance on security policies, procedures, and guidelines related to laptop computers and electronic media.
 - C. Interviewed officials from the Office of the Chief Information Officer regarding IRS security policies, procedures, and guidelines related to laptop computers and electronic media.
- II. Determined the effectiveness of procedures and controls implemented to protect sensitive data on laptop computers and portable electronic media.
 - A. Analyzed the report of 387 incidents of stolen/lost IRS laptop computers and computer devices or lost personally identifiable information from January 2, 2003, to June 13, 2006, received from the CSIRC² and the TIGTA Office of Investigations. For each incident, we:
 1. Identified how the incidents occurred and determined whether the laptop computers contained sensitive information based on the information provided.
 2. Determined whether the incidents were reported to the CSIRC and to the TIGTA Office of Investigations.

¹ Encryption is a method to convert readable text (i.e., plaintext) to unreadable text (i.e., ciphertext) by applying mathematical algorithms and one or more encryption keys. This is generally performed to protect the confidentiality, integrity, and authenticity of data during storage or transmission.

² The CSIRC provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

- B. Selected a judgmental sample of 100 laptop computers from 4 IRS Area Offices.³ Because the IRS maintained over 47,000 laptop computers, we obtained agreement from the Mission Assurance and Security Services⁴ and the Modernization and Information Technology Services⁵ organizations on our sample size and site selection. The four sites visited were the Area Offices in Laguna Niguel, California; Atlanta, Georgia; Salt Lake City, Utah; and Cincinnati, Ohio. We used a judgmental sample because we were not projecting the audit results. The first two site visits were announced weeks in advance; the last two site visits were unannounced due to concerns about giving warning to employees prior to our visits. The samples consisted of those employees who used taxpayer data as part of their official duties.
- C. At the four sites:
1. Interviewed the nine system administrators to identify the products used to encrypt sensitive data stored on laptop computers; the process to set encryption on sensitive files; how the security policies are communicated to employees; and the local policy on portable electronic media, with a focus on flash drives.⁶
 2. Interviewed the 100 employees assigned to the sample of 100 computers to determine the employees' awareness and knowledge of the encryption process; how sensitive information was encrypted on the laptop computers; and whether the employees used self-purchased or Federal Government-issued flash drives and, if they did, asked why and what information was stored on the flash drives and whether the flash drives were encrypted.
 3. Determined whether taxpayer information stored on laptop computers was unencrypted by analyzing the hard drives on the 100 laptop computers.
 4. Evaluated the controls over the protection of the boot process⁷ on the sample of the 100 laptop computers.

³ Area Offices are located throughout the United States; they serve as the coordination point for and assist the public with tax issues.

⁴ The Mission Assurance and Security Services organization supports the vital mission of the IRS by assuring the security and resilience of critical Agency functions and business processes.

⁵ The Modernization and Information Technology Services organization is responsible for providing information technology support and services for the IRS by building and maintaining information systems that will help the IRS achieve its mission, objectives, and business vision.

⁶ A flash drive is an external data storage device that plugs into the computer and emulates a small disk drive. It allows data to be easily transferred from one computer to another.

⁷ The boot process represents the computer's internal process of starting when powered up. This process involves the execution of preset instructions located on the computer's hard drive, including startup of security features of the computer such as password protection.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

- III. Determined the effectiveness of procedures and controls implemented to protect sensitive data on media such as backup media when data are stored at non-IRS offsite facilities. The non-IRS offsite facilities were located fewer than 40 miles from the selected Area Offices.
- A. Assessed the security and encryption placed on backup media that are to be stored at non-IRS offsite facilities.
 - B. Assessed the security of the method of transportation used to ship backup media to non-IRS offsite storage facilities.
 - C. Assessed the adequacy of the physical security controls where the media were stored.
 - D. Reconciled the list of backup media to assess the accuracy and completeness of the written inventory.
 - E. Validated the list of IRS employees authorized to access the non-IRS offsite storage facilities and view tapes.
- IV. Determined the effectiveness of actions taken by the IRS to cleanse sensitive data from electronic media that are to be reused or discarded at the Campuses⁸ in Fresno, California; Atlanta, Georgia; Covington, Kentucky; and Ogden, Utah.
- A. Assessed the procedures used to process laptop computers for disposal and determined whether these procedures meet IRS guidelines.
 - 1. Interviewed responsible staff members and obtained records of actions taken to cleanse sensitive data that might reside on the media before disposal of the equipment, including backup tapes.
 - 2. Obtained a list of the various types of equipment that are cleansed and a description of all the cleansing techniques used and when each type is applicable.
 - 3. Identified where equipment awaiting disposal is stored and the final destination of the disposed equipment.
 - 4. Identified actions taken to remove items from the Information Technology Asset Management Systems, the official IRS computer inventory recordkeeping system.
 - B. Assessed the adherence to disposal procedures and noted any variation or noncompliance. We also verified whether equipment had been cleansed of all readable data.

⁸ 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.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Joseph Cooney, Acting Audit Manager
Midori Ohno, Lead Auditor
Richard Borst, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Jackie Nguyen, Senior Auditor



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

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



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 480 individuals affected (see page 7).

Methodology Used to Measure the Reported Benefit:

Our objective was to determine whether the IRS is adequately protecting sensitive data on laptop computers. We found that employees reported 387 incidents from January 2, 2003, to June 13, 2006, involving the loss or theft of computer equipment and/or sensitive data. Based on the available information for the 387 incidents, we determined at least 24 of the incidents could have been prevented if employees had followed IRS policies and procedures. The 24 incidents involved personally identifiable information for 480 individuals. The loss of these records, which consisted of taxpayer and employee information, also could have been prevented had the incidents not occurred.

Recommendations 3 through 5 should increase awareness and reinforce employee responsibilities on computer security and should decrease the number of incidents that can be prevented by adhering to IRS policies and procedures.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Appendix V

Office of Management and Budget Memoranda

The Office of Management and Budget¹ has issued several memoranda addressing data protection in Federal Government bureaus and agencies.

- M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006). This memorandum reemphasizes the responsibilities of Federal Government agencies regarding laws and policies for safeguarding sensitive personally identifiable information. The memorandum also requires agencies to remind employees of their responsibilities within 30 calendar days of the issuance of this memorandum.
- M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006). This memorandum recommends that four actions to protect sensitive agency data be taken by all agencies: (1) encrypt all data on mobile devices, (2) allow remote access only with 2 separate mechanisms of authentication, (3) use a 30-minute inactivity timeout function for remote access, and (4) log all computer data extracts from databases and ensure data are erased after 90 calendar days unless the data are still needed. The memorandum also provides a checklist for protecting remote information for agencies to complete within 45 calendar days of the issuance of this memorandum.
- M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006). This memorandum requires that all incidents involving personally identifiable information be reported to the United States Computer Emergency Readiness Team² within 1 hour of discovery.
- M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act³ and Agency Privacy Management* (July 17, 2006). This memorandum provides additional instructions and requires additional information for the 2006 Act submission.

¹ The Office of Management and Budget ensures agencies' reports, rules, testimony, and proposed legislation are consistent with the President's budget and administration policies. The Office of Management and Budget's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public.

² The United States Computer Emergency Readiness Team is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, the Team coordinates defense against and response to cyber attacks across the nation.

³ This Act is part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301 (2002). The Federal Information Security Management Act includes protecting information and systems from unauthorized access, use, disclosure, or modification, including controls for disclosure and confidentiality to protect personal privacy.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Appendix VI

Management's Response to the Draft Report




CHIEF INFORMATION OFFICER

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

RECEIVED
MAR 05 2007

March 1, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard A. Spires
Chief Information Officer 

SUBJECT: Management Response to Draft Audit Report –
The Internal Revenue Service Is Not Adequately Protecting Taxpayer
Data on Laptop Computers and Other Portable Electronic Media
Devices – Audit #200620001 (i-Trak #2007-20746)

Thank you for the opportunity to review the draft audit report and respond to the recommendations. Modernization and Information Technology Services (MITS) and Mission Assurance & Security Services (MA&SS) have carefully reviewed the draft report and agree that your recommendations have merit and necessitate corrective action by the Internal Revenue Service (IRS). We have made substantial progress in addressing the findings in your draft report and have implemented several of the recommendations and associated corrective actions.

The IRS is taking aggressive steps to further secure government equipment and protect sensitive data to mitigate the risk of potential identity theft or other fraudulent activity. These actions include:

- Providing IRS employees the capability to encrypt sensitive files and emails on their computers;
- Deploying full disk encryption technology and physical cable locks on all employee laptops, and identifying a secure encryption alternative for tapes exchanged with federal, state, and other partners;
- Implementing a comprehensive communications strategy focused on educating employees on asset and data protection responsibilities, use of encryption capabilities, and reporting losses or thefts; and
- Establishing an executive-level incident management and victim notification program to ensure appropriate handling of losses of sensitive information.

The IRS has reviewed all security and privacy policies and processes to ensure they reflect the new or updated policy directives recently issued by the Office of Management and Budget related to the protection of sensitive information. As a result, we have implemented new processes and issued several new or strengthened data protection policies and procedures.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

2

We are committed to improving the security of sensitive data stored on our laptop computers and other portable electronic media. We have worked closely with the Chief, MA&SS and staff in developing this management response. Our detailed responses to the recommendations in this report are attached.

If you have any questions or feedback, please contact me at (202) 622-6800. Members of your staff may also contact Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

RECOMMENDATION #1: The Chief, Mission Assurance and Security Services, should refine CSIRC reporting and handling procedures to ensure that sufficient details are gathered and recorded in the incident write-ups regarding taxpayers potentially affected by a loss and the nature of the lost data.

CORRECTIVE ACTION #1: We agree with this recommendation. Mission Assurance and Security Services (MA&SS) has refined the incidence handling and reporting procedures to ensure sufficient details are gathered and recorded regarding taxpayers potentially affected by the loss along with the nature of the lost data. These refinements include the stand up of a Personally Identifiable Information (PII) Incidence Response Working Group. Members of this working group include the business units, MA&SS' Computer Security Incidence Response Center (CSIRC), and its Office of Privacy and Information Protection. This working group has developed a PII Incidence Management Policy, PII analysis template, and a risk analysis framework. These efforts have resulted in modifications to the CSIRC intake process and a hand-off of appropriate incidents to the core response group for disposition.

IMPLEMENTATION DATE: Closed September 30, 2006

RESPONSIBLE OFFICIAL: Director, Office of Privacy and Information Protection

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: The Chief, Mission Assurance and Security Services should coordinate with the business units that had reported lost or stolen computer devices since 2003 and quantify the impact to taxpayers in terms of how many taxpayers were affected by the incidents and what personally identifiable information was lost.

CORRECTIVE ACTION #2: We agree with this recommendation. Between July and September 2006, MA&SS launched two efforts to refine existing CSIRC reporting and handling procedures.

For each of the business units that have reported lost or stolen computer devices since 2003, MA&SS has requested a quantification of the impact to taxpayers and a determination of the lost PII. In addition, in response to OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006, CSIRC made modifications to the reporting and handling procedures to capture details regarding the types of data elements, encryption status of each affected asset, and the number of individuals – both taxpayers and non-taxpayers – potentially impacted.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

Moreover, under the leadership of the Chief, MA&SS, the Office of Privacy and Information Protection established a cross-functional working group to ensure the appropriate focus on details involving the data and encryption status of each incident. At the same time, the group ensured that the reporting and incident handling did not violate IRC 6103 or the Privacy Act of 1974. The membership of the working group included subject matter experts from across the IRS, including the Office of Disclosure, Chief Counsel, Labor Relations, CSIRC, and the Office of Privacy and Information Protection.

IMPLEMENTATION DATE: Closed December 30, 2006

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #3: The Chief, Mission Assurance and Security Services should provide employees periodic reminders of their responsibilities for protecting computer devices, which, at a minimum should include storing laptop computers in locking cabinets in the office, storing laptop computers in the trunks of vehicles, and securing laptop computers at home or alternate work locations.

CORRECTIVE ACTION #3: We agree with this recommendation. In response to OMB M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, the Chief, MA&SS tasked the Office of Privacy and Information Protection to establish a strategic communications team to lead an integrated effort reminding employees of their responsibilities regarding the protection of personally identifiable information and assets, including proper storage of laptops. The strategic communications team membership includes experts from the business units, Communications and Liaison, and the Office of Privacy and Information Protection.

Between June 2006 and December 2006, the strategic communications team issued multiple targeted messages to all IRS employees. Employees have also received periodic reminders from MA&SS on their responsibilities for protecting computing devices. In addition, this topic was included in the Information Protection Mandatory Awareness briefing in 2006. This important message will remain a focal point for the communications team and is a standard part of the MA&SS ongoing communications activities.

IMPLEMENTATION DATE: Closed December 30, 2006

RESPONSIBLE OFFICIAL: Director, Office of Privacy and Information Protection

CORRECTIVE ACTION MONITORING PLAN: N/A



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

RECOMMENDATION #4: The Chief, Mission Assurance and Security Services should consider purchasing computer cable locks for employees to provide an additional layer of security at their residence, hotel, or taxpayer site. Instructions should be provided on how to use the locks and the best method to secure the laptop computer to an immobile or heavy object.

RECOMMENDATION #4A: The Chief, Mission Assurance and Security Services should consider purchasing computer cable locks for employees to provide an additional layer of security.

CORRECTIVE ACTION #4A: We agree with the recommendation. Modernization and Information Technology Services (MITS) purchased computer combination cable locks for all laptops on August 31, 2006 and is distributing the locks to all laptop users. At the time of distribution, MITS issued instructions on how to use the lock. Information on using the locks was also posted at http://mits.web.irs.gov/M_HeresTheLatest/LockYourLaptop.htm for employees.

IMPLEMENTATION DATE: April 1, 2007

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, End User Equipment & Services

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4B: Instructions should be provided on how to use the locks and the best method to secure the laptop to an immobile or heavy object.

CORRECTIVE ACTION #4B: We agree with this recommendation. MA&SS issued an interim policy to clarify the use of computer cable locks for employees.

IMPLEMENTATION DATE: Closed November 16, 2006

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #5: The Chief, Mission Assurance and Security Services should periodically publicize an explanation of employees' responsibilities for preventing the loss of computer equipment and taxpayer data, the associated disciplinary penalties for negligence over these responsibilities, and a statistical summary of actual violations and disciplinary actions relating to loss of computer equipment and taxpayer data.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

CORRECTIVE ACTION #5: We agree with this recommendation. As a part of the mandatory annual Information Protection training, MA&SS will explain employees' responsibilities for preventing the loss of computer equipment and taxpayer data and the associated disciplinary penalties for negligence over these responsibilities. Publicizing statistical summaries presents privacy and labor relations issues for the IRS; therefore, MA&SS will implement a communications plan which includes issuing regular announcements to highlight the disciplinary penalties in order to remind employees to be vigilant in protecting personal identifiable information and agency equipment.

IMPLEMENTATION DATE: December 15, 2007

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: Progress will be monitored through periodic reporting to the Security Services and Privacy Executive Steering Committee.

RECOMMENDATION #6: The Chief Information Officer (CIO) should include a reminder in the annual certification of security awareness that employees should store encrypted sensitive information on a secure location of their laptop computers and show them how to use commercial software approved by the IRS to encrypt sensitive data on electronic media devices, such as flash drives.

CORRECTIVE ACTION #6: We agree with this recommendation. The Chief, MA&SS, in conjunction with the Human Capital Office and End User Equipment & Services (EUES), developed and implemented a mandatory Information Protection training module and encryption job aides to remind employees of their responsibility to secure personally identifiable information and how to use available encryption technologies.

During November 2006, all IRS employees took the mandatory Information Protection training. The curriculum included materials on policies governing secure information storage, transmission, and guidance on available encryption technologies. The IRS will review training content on an annual basis and update as needed to ensure compliance with requirements and IRS policies.

In addition to the mandatory training, on October 26, 2006, encryption job aides were developed and pushed to all IRS desktops and laptops. The encryption job aides are a "how to" on use of available encryption technologies: Secure Messaging for email, WinZip for removal media, and Encrypted File System (EFS) for files on the workstation. The EFS customer installation and operation guide is also available to all users at http://mits.web.irs.gov/m_communications/protectdata1.htm#1. WinZip 9.0 instructions are available at http://mits.web.irs.gov/m_communications/protectdata1.htm#2.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

IMPLEMENTATION DATE: Closed January 1, 2007

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #7: The Chief Information Officer should require front-line managers to periodically check their employees' laptop computers to ensure encryption solutions are being used by employees and sensitive data are encrypted properly.

CORRECTIVE ACTION #7: We agree with this recommendation. The IRS mandated for all laptop users the implementation of disk encryption, which ensures the entire drive is encrypted. Coupled with the disk encryption process, MA&SS will issue a policy requiring all employees to annually certify that they are using encryption tools properly to protect sensitive data.

IMPLEMENTATION DATE: October 15, 2007

RESPONSIBLE OFFICIAL: Director, Information Technology Security

CORRECTIVE ACTION MONITORING PLAN: Progress will be monitored through periodic reporting to the Security Services and Privacy Executive Steering Committee.

RECOMMENDATION #8: The Chief Information Officer should consider implementing a systemic disk encryption solution on laptop computers. By encrypting the entire hard drive, employees will no longer have to determine what data needs to be encrypted. This solution will supplement the two existing encryption solutions previously discussed.

CORRECTIVE ACTION #8: We agree with this recommendation. The IRS implemented a systemic disk encryption, which resulted in a mandate for all laptop users to install the enterprise disk encryption solution. This solution encrypts the entire hard drive and requires access authentication, via login and password, whenever the laptop has been turned off. If the laptop is lost or stolen, unauthorized users will not be able to access any data on the hard drive.

IMPLEMENTATION DATE: April 1, 2007

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, End User Equipment & Services

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #9: The Chief Information Officer should require system administrators, when servicing a laptop computer, to check the boot process settings to ensure



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

the boot process password is enabled and the boot order lists only the hard drive as the boot initiation process. System administrators should document completion of this task.

CORRECTIVE ACTION #9: We agree with this recommendation. The Chief Information Officer will issue a memorandum that requires all workstation administrators, when servicing a laptop computer, to document the correct boot process settings (password is enabled and the hard drive is the boot initiation process location) via the Enterprise Workstation Check List. Moreover, with the addition of enterprise disk encryption, the boot initiation process is relegated to the hard drive by individuals who possess a disk encryption access profile resident on the workstation.

IMPLEMENTATION DATE: June 1, 2007

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, End User Equipment & Services

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #10: The Chief Information Officer should implement procedures to encrypt backup data sent to non-IRS facilities.

CORRECTIVE ACTION #10: We agree with this recommendation. Enterprise Operations (EOPS) will analyze, test, procure, and implement a software-based automated encryption solution to work in conjunction with existing backup technology for servers. In support of mainframe configurations, the IRS will execute a proof of concept test, which includes the use of encryption tape drives along with encryption appliance technology, to identify the most effective encryption method. Testing will conclude in late Fiscal Year (FY) 2007 and formal materials associated with test findings and technical recommendations will be used to develop detailed plans for implementation of encryption in FY08. In addition, WinZip 9.0 is the current encryption software that the IRS requires installed on removable media, such as flash drives. Instructions for how to use WinZip 9.0 are available to users at http://mits.web.irs.gov/m_communications/protectdata1.htm#2.

IMPLEMENTATION DATE: April 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #11: The Chief Information Officer should ensure employees who are assigned oversight responsibilities for non-IRS facilities complete the following tasks:

- Conduct and certify an annual inventory validation of back-up media.



*The Internal Revenue Service Is Not Adequately Protecting
Taxpayer Data on Laptop Computers and Other Portable
Electronic Media Devices*

Attachment

Draft Report – The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices – Audit #200620001 (i-Trak #2007-20746)

- Conduct periodic checks to verify the accuracy of the access list and those individuals who no longer have a need to access the non-IRS facilities have been removed.
- Conduct an annual internal physical security review of the non-IRS off-site facility to determine that the site meets IRS requirements.

CORRECTIVE ACTION #11: We agree with this recommendation. The CIO will review and update the IRM 2.7.4 to ensure oversight responsibilities are clearly defined for the annual inventory validation of back-up media, for periodic checks of accurate facilities access lists, and for annual physical security reviews.

To monitor compliance:

1. EUES' Tax Processing Operations Support will perform an inventory validation of all back-up magnetic media for the 10 campus locations stored in the offsite facilities. EOPS will continue to conduct a physical inventory of magnetic media, including a physical review of all tapes contained in IRS Computing Center locations, each year.
2. Representatives from MITS, Agency Wide Shared Services (AWSS), and MA&SS will conduct a representative sample check to verify the accuracy of the access list and to ensure individuals who no longer need access to the non-IRS facility are removed. EOPS will continue to perform an annual review of access lists.
3. Representatives from MITS, AWSS, and MA&SS will conduct a representative sample of the non-IRS off-premise storage sites to determine that the site meets IRS physical security requirements. EOPS will continue to conduct regular security reviews of off-site storage facilities used in support of Computing Center operations.

IMPLEMENTATION DATE: December 1, 2007

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, End User Equipment & Services

CORRECTIVE ACTION MONITORING PLAN: N/A