Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices

August 31, 2009

Reference Number: 2009-20-120

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

Phone Number | 202-622-6500
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 31, 2009

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Nancy A. Nakamura

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

SUBJECT: Final Audit Report – Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices (Audit # 200820025)

This report presents the results of our review to follow up on a prior audit report[1] and determine whether the Internal Revenue Service (IRS) is adequately protecting sensitive data on laptop computers and other portable electronic media devices. We also evaluated the controls over incident reporting and backup data. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and is part of our statutory requirement to annually review the adequacy and security of IRS technology.

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. While the IRS has made significant improvements to protect sensitive data on laptop computers and other portable electronic media devices, controls over incident reporting and backup data require additional improvements. As a result, taxpayers may not be notified when security incidents involving their personal data have occurred and taxpayer data may be at risk of theft and unauthorized disclosure.

[1] *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).

Synopsis

The IRS has effectively implemented encryption technologies on laptop computers and other portable storage devices. These systemic encryption solutions have strengthened the protection of taxpayer data and personally identifiable information and have reduced the chance of unauthorized disclosure of sensitive data when laptop computers and other portable electronic media are lost or stolen. The IRS has also taken actions to assist employees with securing laptop computers and sensitive data by purchasing cable locks for laptop computers, implementing a comprehensive training strategy that instructs employees on the process for reporting lost or stolen items, and informing employees of their responsibilities for securing sensitive data.

Although the IRS has made significant improvements relating to controls over electronic media and the protection of sensitive data, we identified two areas where continued diligence is needed. First, processes for tracking security incidents could be enhanced to ensure that all incidents are properly handled. During our prior review, we identified inadequate coordination between the IRS Computer Security Incident Response Center[2] and the Treasury Inspector General for Tax Administration Office of Investigations[3] to ensure proper reporting of security incidents. During this review, the number of reported incidents known by both the Computer Security Incident Response Center and the Office of Investigations had significantly increased to 96 percent of all related incidents, although we found incidents relating to hard copy losses that were not shared between both organizations. We believe all incidents should be reported in a timely manner and shared between all affected organizations. The timely reporting and sharing of incident information enables the IRS to continue to meet incident reporting time periods, fulfill taxpayer notification requirements, and apply consistent disciplinary actions for employee negligence.

Second, the IRS needs to enforce controls for protecting backup data from unauthorized disclosure and ensuring its availability in the event of a disaster. During our prior review, the IRS was not encrypting backup data that were sent to offsite storage facilities, was not performing annual inventory validations of the backup data, and was not always performing periodic reviews of the approved access list of employees authorized to access the offsite storage facilities. During this review, we found that the IRS had revised its processes and procedures and no longer required field offices to send its backup data to offsite facilities. We confirmed that the two field offices we visited had implemented the new procedures to transmit their

[2] The IRS Computer Security Incident Response Center is responsible for ensuring security incidents are reported to the Treasury Computer Security Incident Response Center, which serves as the central point of contact for escalating incidents reported by its bureaus to the United States Computer Emergency Readiness Team, in compliance with stringent time periods, and for funneling incidents involving potential loss of personally identifiable information to the IRS Office of Privacy, Information Protection, and Data Security for a determination of whether taxpayers must be contacted regarding compromised data.

[3] The Office of Investigations is responsible for investigating all incidents to determine if employee negligence was involved and, if found, to provide a report to the IRS Human Capital Office.

backup data through the IRS secured network to an IRS Computing Center,[4] where they were encrypted before being sent to an offsite storage facility.

However, we visited one of the three IRS Computing Centers charged with controlling IRS backup data and found that the annual inventory validation of the backup data at the offsite facility was not conducted. In addition, the access list of IRS employees authorized to access the data at the offsite facility had not been recently validated and 15 individuals who no longer had a business need had access to the backup data. The IRS indicated these weaknesses were caused by management turnover and a lack of management oversight over backup procedures.

Recommendations

The Chief Technology Officer should ensure that 1) the IRS collaborates with the Treasury Inspector General for Tax Administration to revise the Memorandum of Understanding to ensure all incidents involving personally identifiable information in electronic or hard copy form are properly reported and shared between the IRS Computer Security Incident Response Center and the Treasury Inspector General for Tax Administration Office of Investigations, and 2) all backup data are properly protected from unauthorized access and disclosure.

Response

IRS management agreed with the recommendations. The IRS Computer Security Incident Response Center will collaborate with the Treasury Inspector General for Tax Administration Office of Investigations; the Office of Privacy, Information Protection, and Data Security; and the IRS Office of Disclosure to revise the Memorandum of Understanding to better represent the current environment of incident reporting and sharing. The Enterprise Operations organization will initiate consolidation of media management into one organization to ensure consistency in media management and policy. The Modernization and Information Technology Services organization will ensure media management controls are in place to protect backup data from unauthorized access and disclosure. Management's complete response to the draft report is included as Appendix IV.

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

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, Acting Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
MOU	Memorandum of Understanding
OI	Office of Investigations
PIPDS	Office of Privacy, Information Protection, and Data Security
TIGTA	Treasury Inspector General for Tax Administration

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 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.

Most IRS employees use taxpayer information within IRS facilities to carry out their responsibilities; 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 outside of IRS facilities when conducting reviews with business taxpayers. When taxpayer information is taken outside of the office, 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 in a place that is not visible from outside of the vehicle.
- Encrypting[1] taxpayer data on computer devices – Even if a computer device is lost or stolen, the data are still protected if they were encrypted. Encryption ensures that 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 during the computer startup process.[2] However, this control can sometimes be bypassed if the computer is not properly configured.

[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] This process represents a computer's internal process of starting up when it is powered up. The 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.

- 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 determine whether taxpayer data have been compromised.

In addition, data that are backed up and stored offsite so that operations can be restored in the event of a disaster may also be at risk.[3] 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 adequate data accountability and protection from unauthorized access.

Since 2003, we have conducted at least three reviews that included assessing controls over sensitive data on laptop computers and other portable electronic media. These reviews found internal control weaknesses in the IRS' safeguarding of taxpayer data.[4]

This review was performed at IRS offices in Jacksonville, Florida; New Carrollton, Maryland; Oklahoma City, Oklahoma; and Memphis, Tennessee, during the period September 2008 through April 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[3] 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.

[4] *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007); *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 22, 2006); and *Security Over Computers Used in Telecommuting Needs to Be Strengthened* (Reference Number 2003-20-118, dated July 1, 2003).

Results of Review

Actions Have Been Taken to Increase the Protection of Sensitive Data

In March 2007, we reported[5] that sensitive data were not encrypted on laptop computers and other electronic media and that access controls were incorrectly configured and could be circumvented to gain access to unencrypted sensitive data. In addition, we reported that physical security was not adequate over computer equipment. We found that laptop computers overwhelmingly represented the largest category of lost or stolen items each year, and employees who were negligent for the losses or thefts were rarely disciplined. These deficiencies made the IRS vulnerable to unauthorized disclosure of taxpayer data and loss of personally identifiable information, both of which can be used for identity theft purposes. The IRS implemented the recommendations from this prior report, resulting in increased protection of sensitive data.

In addition, one of the recommendations from our prior report dealt with implementing a systemic disk encryption solution on laptop computers. This solution, also known as hard disk encryption, encrypts the entire hard drive and requires access authentication whenever the laptop computer is operational. The IRS agreed with the recommendation and replied that it would implement an enterprise-wide hard disk encryption solution for its laptop computers.

During this review, the IRS provided us with documentation reflecting that 99 percent of its laptop computers contained the hard drive encryption program. During our review of 100 laptop computers in 4 IRS offices, we confirmed that all 100 laptop computers had the hard disk encryption software installed and that the software was functioning as intended. This solution dramatically improved the protection of sensitive data on laptop computers and resolved the access control deficiencies cited in our prior report. Only after a successful logon to the encryption software will the computer start the logon process to access other system files. Consequently, any sensitive data on the computer remains encrypted until a user has successfully logged on and deactivated the encryption.

Because files on the hard drive are no longer encrypted after a laptop computer has been turned on, the IRS still requires employees to encrypt sensitive files on a laptop computer using the Microsoft Windows Operating System encryption program, also known as the Encrypting File

[5] *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).

System.[6] During this review, we found that 23 of 100 laptop computers had unencrypted sensitive files that could be accessed by anyone who logged on to the laptop computer after the hard disk encryption had been deactivated. These files represent taxpayer data, such as Social Security Numbers or Taxpayer Identification Numbers on various tax forms, as well as personally identifiable data of the employee. While these results represent an improvement over our prior audit results where 44 of the 100 laptops tested were noncompliant, the IRS should remain diligent in reinforcing use of its encryption technologies through its annual security training and periodic reminders to employees. We believe the risk of this issue is lessened by the hard drive encryption previously discussed, which protects all files when the laptop computer is turned off.

In addition to the hard disk encryption, the IRS has implemented an encryption solution over data that are transferred to an external media outlet, such as a removable media storage device or computer disk. We confirmed that the encryption solution was installed on all 100 laptop computers we reviewed. These systemic encryption solutions have strengthened the protection of taxpayer data and personally identifiable information at the IRS, and the encryption solutions have reduced the chance of unauthorized disclosure of sensitive data when portable electronic media devices are lost or stolen.

The IRS has also taken actions to assist employees with securing laptop computers and sensitive data. One of the recommendations in our prior report dealt with the purchase of cable locks for computers and providing employees with related security awareness training. The IRS completed these corrective actions. During our review of the 100 laptop computers, we found that 99 employees used cable locks to secure their laptop computers and 96 employees had received training or instructions on how to secure laptops, use encryption, and report lost or stolen laptops.

IRS employees reported a total of 866 incidents during the period June 14, 2006, to September 17, 2008. We categorized the 866 incidents by item type and found that laptop computers continued to represent the largest number of incidents (270 incidents) of lost or stolen items. Laptop computers are attractive targets for thieves. No organization is impervious to theft or loss of devices containing sensitive data, especially an organization as large as the IRS, with approximately 100,000 employees and more than 40,000 laptop computers. The IRS has informed employees of their responsibilities for securing sensitive data and the penalties associated with negligence.[7] In April 2008, the IRS implemented procedures for tracking employee negligence cases to ensure that all are consistently processed and appropriate penalties

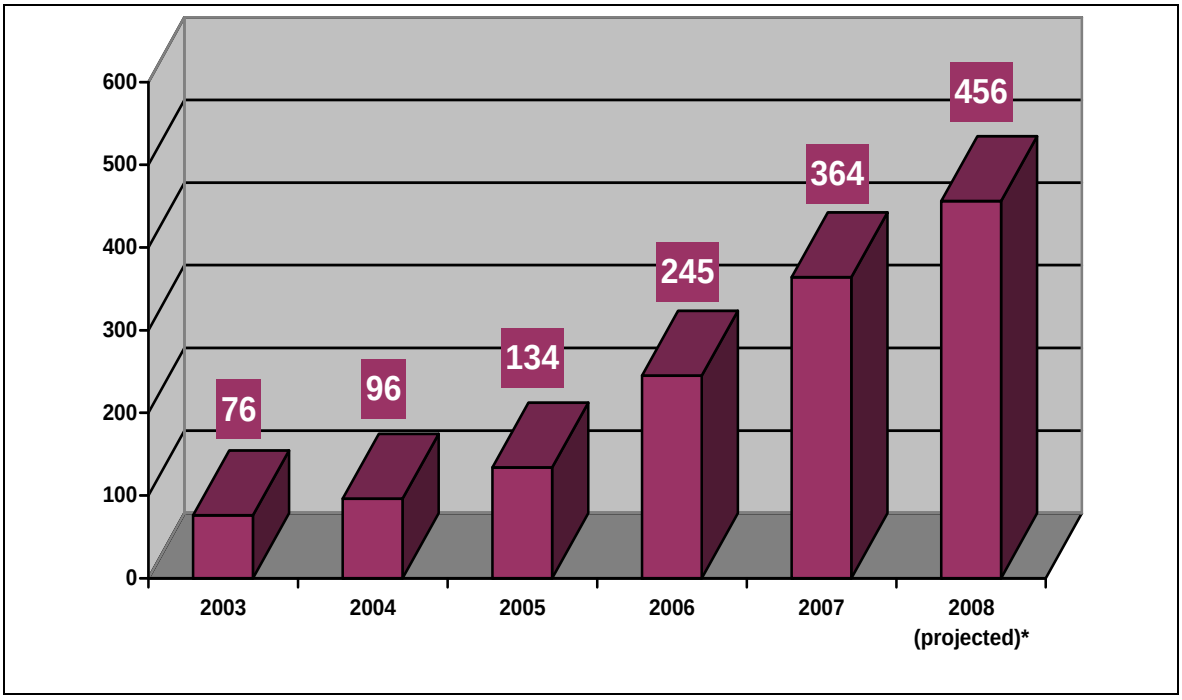
[6] Under the Encrypting File System, laptop computers are configured to encrypt data residing in specific file folders on the hard drive. Employees need only to save sensitive files to these file folders and the computer will automatically encrypt the files.

[7] Negligence is the failure to exercise that degree of care that would have been exercised by a reasonable person under the same circumstances.

are applied. During this review, we determined that 152 of the 866 incidents involved employee negligence and could have been prevented if the employees had followed IRS policies and procedures. Nineteen of the 152 incidents occurred since April 2008. We reviewed these 19 incidents to determine whether the new disciplinary processes were effective. We were encouraged to find that 17 of the 19 incidents were being processed in accordance with the newly implemented procedures. However, most of these incidents were still under investigation during the time of our review, and we were unable to make a reliable evaluation on the effectiveness of the new procedures.

The number of reported incidents relating to lost or stolen media potentially containing sensitive taxpayer and employee data continued to increase from Calendar Year 2003 to Calendar Year 2008, as illustrated by Figure 1.

Figure 1: Number of Incidents of Theft or Loss of Computer Equipment and/or Taxpayer Data Per Year



* We obtained incidents through September 17, 2008, and made a projection through the end of Calendar Year 2008 using a direct proportional ratio.
Source: Our analysis and projection based on IRS Computer Security Incident Response Center and Treasury Inspector General for Tax Administration Office of Investigations data.

We believe this upward trend is due, in part, to the increased reporting of incidents by IRS employees. Based on recommendations from our prior report, the IRS implemented a comprehensive training strategy that instructed employees on the process for reporting lost or

stolen items. In Calendar Year 2006, the IRS provided additional guidance to employees to report lost or stolen sensitive data within 1 hour of the incident, in compliance with new Federal Government reporting requirements. As a result of the 1-hour reporting rule, we noted that current statistics likely included incident reports of lost or stolen items that were subsequently recovered. Employees may not have reported these incidents under previous reporting guidelines.

According to a Calendar Year 2008 survey by the Computer Security Institute,[8] theft of laptops or other mobile devices was the third most frequently occurring incident (42 percent) at respondents' organizations. In addition, the survey found that the cost of the loss of customer or employee confidential data averaged $268,000 per incident. Therefore, the loss of a laptop computer may be quite expensive if it contains unencrypted sensitive data. Replacing lost or stolen laptops that were encrypted generally does not cost more than the replacement and associated administrative costs. While we have some concerns with the upward trend of overall incidents, we believe the IRS has effectively mitigated much of the risk of unauthorized disclosure of sensitive data by systemically encrypting the data on laptop computers and other electronic devices.

Although Controls Have Improved, Additional Steps Could Be Taken to Expand the Reporting of Incidents and the Protection of Sensitive Data

While the IRS has made significant improvements relating to controls over electronic media and the protection of sensitive data, continued diligence is necessary to ensure taxpayer data are fully protected. We identified two areas where the IRS could take actions to improve the protection of sensitive data. First, processes for tracking reported security incidents between organizations need improvement to ensure that all affected organizations receive and exchange information related to the incident in a timely manner. Second, the IRS needs to enforce controls for protecting backup data from unauthorized disclosure and ensuring its availability in the event of a disaster. As a result of deficiencies in these areas, taxpayers may not be notified when security incidents involving their personal data have occurred and taxpayer data may be at risk of theft and unauthorized disclosure.

[8] The *2008 CSI Computer Crime and Security Survey*, by Robert Richardson, Director of Computer Security Institute, was based on the responses of more than 500 computer security practitioners from government and private institutions. According to the survey, virus incidents occurred most frequently (49 percent) at respondents' organizations in 2008. Insider abuse of networks was the second-most frequently occurring incident (44 percent).

Incident reporting controls could be enhanced to ensure better tracking and processing of incidents

The Office of Management and Budget requires Federal Government agencies to report all incidents involving personally identifiable information, in electronic or hard copy form, to the United States Computer Emergency Readiness Team within 1 hour of discovering the incident, without taking the time to distinguish between suspected and confirmed security breaches. In order to comply with Federal regulations, IRS employees are required to report security incidents immediately upon identification, not to exceed 1 hour, to 1) the employee's immediate manager, 2) the IRS Computer Security Incident Response Center (CSIRC), and 3) the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI). The CSIRC is responsible for reporting the incidents to the Treasury Computer Security Incident Response Center, which serves as the central point of contact for escalating incidents reported by its bureaus to the United States Computer Emergency Readiness Team, meeting the stringent reporting time periods set by the Office of Management and Budget.

The CSIRC is also responsible for directing incidents involving potential loss of personally identifiable information to the IRS Office of Privacy, Information Protection, and Data Security (PIPDS). Lost or compromised personally identifiable information may be used to perpetrate identity theft or other forms of fraud if the information falls into unauthorized hands. Personally identifiable information is information in either electronic or hard copy format that can be used to distinguish or trace an individual's identity, such as an individual's name, Social Security Number, Individual Taxpayer Identification Number, or address.

The PIPDS manages the process within the IRS to notify individuals who are at high risk of harm following a loss of personally identifiable information. The affected individuals are notified without unreasonable delay following a risk assessment of the incident. The IRS sends a concise notification to affected individuals, which includes free credit monitoring services for 1 year and other useful information and contacts to assist the taxpayer in protecting themselves from harm. For example, from October 1, 2006, to September 17, 2008, the PIPDS identified 132 incidents for which the risk of identify theft or other harm was likely, and sent notification letters to 17,498 potentially affected taxpayers.

The TIGTA OI is responsible for investigating all incidents to determine whether employee negligence was involved and, if found, to provide a report to the IRS Human Capital Office. Based on the OI report and the pertinent facts of the case, the Human Capital Office works with the employee's respective manager to determine the appropriate penalty. It also tracks the disciplinary actions taken against negligent employees.

During our prior review, we identified inadequate coordination between the IRS CSIRC and the TIGTA OI to ensure proper reporting of security incidents. We found that IRS employees did not consistently report security incidents to both the CSIRC and the OI as required by IRS policy. As a result, of the 387 incidents that occurred from January 2, 2003, to June 13, 2006,

the CSIRC was aware of 91 (24 percent) incidents and the OI was aware of 296 (76 percent) incidents. Of the incidents that each organization was aware of, the CSIRC shared 42 incidents with the OI, and the OI did not share any incidents with the CSIRC.

To correct this condition, the CSIRC and the OI entered into a Memorandum of Understanding (MOU), effective December 28, 2006, that defined their joint responsibilities for tracking and sharing computer security incidents involving the loss or theft of information technology assets.[9] Each organization was to monitor reported incidents in separate tracking systems, assign case numbers, provide automated notification of received incident reports to the other organization, and perform monthly reconciliations of the incident reports received to ensure all incidents were properly documented.

Our current review found that the number of reported incidents known by both the CSIRC and the OI significantly increased. From January 1, 2007, to September 17, 2008, 535 incidents occurred that were required to be shared under the MOU. Of the 535 incidents, the CSIRC was aware of 515 (96 percent) and the OI was aware of 514 (96 percent). We attribute this significant improvement to the IRS informing employees of their responsibilities for reporting incidents and to the CSIRC and OI implementation of automated notification of received incidents to each other in accordance with the MOU.

However, we believe additional improvements are needed to ensure all incidents are known by both the CSIRC and the OI so that all incidents are properly addressed. Of the 535 incidents, the OI was unaware of 21 incidents that were in the CSIRC tracking system. The OI determined that the CSIRC had not sent automated notification for 7 of these 21 incidents, and that the OI had not captured 14 incidents that the CSIRC had sent. Incidents that are not captured by the OI may not be evaluated for employee negligence or investigative purposes.

Of the 535 incidents, the CSIRC was unaware of 20 incidents that were in the OI tracking system. The CSIRC determined that the OI had not sent automated notification for 18 of these 20 incidents, and the CSIRC had not captured 2 incidents that the OI had sent. Incidents that were not captured by the CSIRC may not meet reporting deadlines or may not be routed to the PIPDS for determination of whether taxpayers should be notified.

The MOU required the CSIRC and the OI to collaboratively perform reconciliations of their separate tracking systems to ensure that all incidents had been captured by both organizations. However, neither the CSIRC nor the OI were performing such reconciliations to identify incidents that had not been shared. During our review, we found that the two tracking systems do not have a common case identifier, making it very difficult and tedious to perform a reconciliation. The CSIRC assigns a unique case identifier to each incident it receives, and the OI assigns a complaint number. The CSIRC modified its tracking system to capture the OI

[9] Information technology assets include desktop computers, laptop computers, servers, Blackberries, CD/DVD, flash drives, floppy discs, and other portable media.

complaint number when inputting cases sent by the OI. However, differences in the case data that the CSIRC and the OI record and timing differences for when automated notifications are sent and when case and complaint numbers are assigned, make it difficult to match cases in the two tracking systems and to reconcile differences.

In addition, the MOU required sharing only the loss or theft of information technology assets, which left some important incidents unshared. For example, we identified 85 incidents involving the loss of taxpayer data in hard copy format that occurred during the period the MOU was in effect and, therefore, were not required to be shared between the CSIRC and the OI. Of these 85 incidents, the CSIRC tracking system contained 63 incidents that were not in the OI tracking system, and the OI tracking system contained 22 incidents that were not in the CSIRC tracking system. Therefore, these 22 incidents were not sent to the PIPDS for review to determine whether taxpayers should be notified. In general, the loss of hard copies that contain taxpayer data are of higher risk than the loss of computer equipment because hard copies are not encrypted. The PIPDS must also ensure taxpayers are timely informed and offered assistance in these instances.

Continued efforts are needed to ensure that all security incidents are captured by both organizations to properly address and reconcile incident reporting. Limiting the type of incidents to share and not reconciling all incidents known by each organization may prevent the IRS from meeting incident reporting time periods, fulfilling taxpayer notification requirements, and applying consistent disciplinary actions for employee negligence.

Management Actions: Subsequent to completion of our fieldwork, the IRS CSIRC and the TIGTA OI met to collaborate on a solution and agreed that the MOU needed revision to better represent the current environment of incident reporting. Possible revisions include developing a better definition of what constitutes personally identifiable information (i.e., inclusion of hard copy records) and enhancing the reporting process by using a common identifier to ensure transparent reporting. The discussion included consideration of designating the CSIRC as the central point of contact in order to reduce employee burden for making three contacts when an incident occurs, and to better ensure the CSIRC can fulfill the 1-hour reporting requirement.

Controls over backup data have improved but require additional enhancements to fully protect taxpayer data

The IRS requires that data at each of its offices be backed up to facilitate business resumption efforts in the event of a disaster. This backup data should be stored offsite to ensure its availability and be encrypted to protect against unauthorized disclosure. To further protect this backup data, the IRS requires that all IRS offices conduct an annual inventory of their backup data to guarantee all data are properly accounted for and to periodically validate the list of employees who are authorized to access the backup data at offsite storage facilities to ensure its protection.

During our prior review, the IRS was not encrypting backup data that were sent to offsite storage facilities. In addition, the IRS was not performing annual inventory validations of the backup data and was not always performing periodic reviews of the approved access list of employees authorized to access the offsite storage facilities. We recommended that the IRS encrypt backup data prior to it being sent offsite and conduct the annual inventory validations and verifications of employees on access lists as required. The IRS agreed with our recommendations.

During this review, we found that the IRS revised its processes and procedures and no longer required some offices to send their backup data to offsite facilities. The new procedures require field offices to electronically transmit their backup data through a secured network to one of three IRS Computing Centers.[10] The Computing Centers then encrypt the backup data prior to sending the data to offsite storage facilities. We confirmed that the two field offices we visited had implemented the new procedures to transmit their backup data through the IRS secured network to the Computing Center, where they were encrypted before being sent to offsite storage.

To follow up on the backup issues at offsite facilities, we visited one of the three IRS Computing Centers charged with controlling IRS backup data. We confirmed that the data were encrypted prior to being sent to offsite storage. However, the IRS did not conduct the annual inventory validation of the backup data at the offsite facility. We selected 30 computer tapes from the inventory listing and physically accounted for all of the tapes. In addition, the IRS had not validated the access list of IRS employees authorized to access the backup data at the offsite facility since December 2007. As a result, we identified 15 individuals on the access list who no longer had a business need to have access to the backup data at the offsite facility.

Lastly, the one headquarters office we visited was not sending its backup data offsite or securing it as required. The data were being maintained onsite, leaving them vulnerable to the same disaster that potentially could disable the headquarters office. While this issue did not specifically involve the protection of backup data from unauthorized individuals, it could potentially affect the availability of the data if a disaster occurs at that headquarters office.

The IRS indicated these weaknesses were caused by management turnover (including retirement, reassignment, and promotion of managers) and a lack of management oversight over backup procedures. These backup data inventory and access weaknesses increase the risk that sensitive data, including personally identifiable information, could be lost or stolen from offsite storage facilities. In addition, not storing backup data securely or at an alternative location puts the data at risk of being permanently destroyed in the event of a disaster.

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

Recommendations

The Chief Technology Officer should ensure that:

Recommendation 1: The IRS collaborates with the TIGTA to revise the MOU to ensure that all incidents involving personally identifiable information in electronic or hard copy form are properly reported and shared between the IRS CSIRC and the TIGTA OI.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS CSIRC will collaborate with the TIGTA OI, the PIPDS, and the IRS Office of Disclosure to revise the MOU to better represent the current environment of incident reporting and sharing.

Recommendation 2: All backup data are properly protected from unauthorized access and disclosure. Specifically, IRS offices should 1) follow policies and procedures for sending backup data to designated locations, 2) conduct annual inventory reconciliations of stored backup media at all offsite storage facilities in accordance with IRS policy, and 3) validate lists of IRS employees authorized to access the backup data at offsite storage facilities when changes occur or at least annually.

> ***Management's Response:*** The IRS agreed with this recommendation. To ensure consistency in media management policies and procedures, the Enterprise Operations organization will initiate consolidation of media management into one organization. The Modernization and Information Technology Services organization will also ensure backup media is properly protected from unauthorized access and disclosure by ensuring media management controls and encryption are in place. In addition, the Modernization and Information Technology Services organization will follow policies and procedures for sending and maintaining backup data to designated offsite storage facilities and will schedule and conduct regular offsite storage facility reconciliations as documented in IRS procedures and validate the authorized access list on an annual basis.

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 other portable electronic media devices. The audit focused on the security of laptop computers and the encryption[1] of sensitive data maintained on laptop computers. We also evaluated the controls over incident reporting and the storage methods for backup tapes at non-IRS offsite facilities.

To accomplish our objectives, we:

I. Determined the effectiveness of procedures and controls implemented to protect sensitive data on laptop computers and other portable electronic media.

A. Analyzed the reporting of 866 incidents involving the loss or theft of electronic devices or hard copy documents from June 14, 2006, to September 17, 2008, received from the IRS CSIRC[2] and the TIGTA OI.[3] For each incident, we:

1. Identified how the incident occurred and determined whether the laptop contained sensitive information based on the information provided.

2. Determined whether the incident was reported to the CSIRC and the OI.

B. Selected a judgmental sample of 100 laptop computers from 4 IRS Area Offices. The four sites visited were Oklahoma City, Oklahoma; Jacksonville, Florida; Memphis Computing Center, Memphis, Tennessee; and New Carrollton, Maryland. We used a judgmental sample because we were not projecting the review results.

C. At the four sites, we:

1. Interviewed the 100 employees to which the sample of 100 computers were assigned to determine whether employees used cable locks to protect their

[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 is responsible for ensuring security incidents are reported to the United States Computer Emergency Response Team, in compliance with stringent time periods and for funneling incidents involving potential loss of personally identifiable information to the IRS PIPDS for a determination of whether taxpayers must be contacted regarding compromised data.
[3] The OI is responsible for investigating all incidents to determine if employee negligence was involved and, if found, to provide a report to the IRS Human Capital Office.

computers and whether they recalled receiving encryption and incident reporting training.

2. Determined whether taxpayer information stored on laptop computers was unencrypted by analyzing the hard drives on the 100 laptop computers.

3. Evaluated the controls over the protection of the startup process[4] on the sample of 100 laptop computers.

II. Determined the effectiveness of procedures and controls implemented to protect sensitive data on media such as backup media.

A. Assessed the security and encryption placed on backup media that are to be stored at a non-IRS offsite facility.

B. Assessed the adequacy of the physical security controls where the media were stored.

C. Reconciled the list of backup media to assess the accuracy and completeness of the written inventory.

D. Judgmentally selected 30 computer tapes from the inventory listing at 1 IRS Computing Center[5] and physically accounted for all of the tapes. We used a judgmental sample because we were not projecting the results of the review and were unable to readily determine the total number of computer tapes stored at the facility.

E. Validated the list of IRS employees authorized to access the facility and the data.

[4] This process represents a computer's internal process of starting up when it is powered up. The 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.

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

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Systems Technology Services)
Kent Sagara, Acting Director
Jody Kitazono, Acting Audit Manager
Alan Beber, Senior Auditor
Charles Ekunwe, Senior Auditor
George Franklin, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Linda Screws, Senior Auditor
Louis Zullo, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Information Officer OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Director, Cybersecurity Programs and Policies OS:CTO:C:PP
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 Technology Officer OS:CTO
    Associate Chief Information Officer, Cybersecurity OS:CTO:C

Appendix IV

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

RECEIVED
AUG 7 - 2009

August 7, 2009

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices (Audit # 200820025) (i-trak #2009-61930)

Thank you for the opportunity to review and respond to the subject audit report. We appreciate your comments and observations that the IRS has effectively implemented encryption technologies on laptop computers and other portable storage devices. The Service has also taken actions to assist employees with securing laptop computers and sensitive data by purchasing cable locks for laptop computers, implementing a comprehensive training strategy instructing employees about the process for reporting lost or stolen items and informing employees of their responsibilities for securing sensitive data.

We acknowledge that our continued diligence is necessary to ensure taxpayer data are fully protected. We agree with the two recommendations made as a result of your audit and the attachment to this memo details our planned actions to implement them.

Your continued support and the guidance your team provides is valuable to us. If you have any questions, please contact me at (202) 622-6800 or Barbara Williams, Program Oversight, at (202) 283-4163.

Attachment

Attachment

Draft Audit Report – Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices (#Audit 200820025) (i-trak #2009-61930)

RECOMMENDATION #1: The Chief Technology Officer should ensure that the IRS collaborates with the TIGTA to revise the Memorandum of Understanding to ensure that all incidents involving personally identifiable information in electronic or hard copy form are properly reported and shared between the IRS Computer Security Incident Response Center and the TIGTA Office of Investigations.

CORRECTIVE ACTION #1: We agree with this recommendation. The IRS Computer Security Incident Response Center will collaborate with the TIGTA Office of Investigations, the IRS Office of Privacy, Information Protection, and Data Security and the IRS Office of Disclosure to revise the Memorandum of Understanding to better represent the current environment of incident reporting and sharing.

IMPLEMENTATION DATE: February 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer for Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should ensure all backup data are properly protected from unauthorized access and disclosure. Specifically, IRS offices should 1) follow policies and procedures for sending backup data to designated locations, 2) conduct annual inventory reconciliations of stored backup media at all offsite storage facilities in accordance with IRS policy, and 3) validate lists of IRS employees authorized to access the backup data at offsite storage facilities when changes occur or at least annually.

CORRECTIVE ACTION #2: We agree with this recommendation. To ensure consistency in media management policies and procedures, the Enterprise Operations organization will initiate consolidation of media management into one organization. The MITS organization will also ensure backup media is properly protected from unauthorized access and disclosure by ensuring media management controls and encryption are in place. In addition, MITS will follow policies and procedures for sending and maintaining backup data to designated offsite storage facilities and will schedule and conduct regular off-site storage facility reconciliations as documented in IRM 2.7.5 and validate the authorized access list with the Contracting Officer Technical Representative on an annual basis.

IMPLEMENTATION DATE: July 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer for Enterprise Operations

Attachment

Draft Audit Report – Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices (#Audit 200820025) (i-trak #2009-61930)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.