Efforts Have Been Made, but Manager and Employee Noncompliance With Security Policies and Procedures Puts Personally Identifiable Information at Risk

August 13, 2007

Reference Number: 2007-20-117

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

August 13, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Efforts Have Been Made, but Manager and Employee Noncompliance With Security Policies and Procedures Puts Personally Identifiable Information at Risk (Audit # 200620007)

This report presents a summary of significant actions that have been accomplished by the Internal Revenue Service (IRS) and the security weaknesses identified in our prior audit reports issued during Fiscal Years 2003 – 2007. The overall objective of this review was to determine the progress the IRS has made in ensuring the security and privacy of personally identifiable information (PII) it maintains. The Consolidated Appropriations Act of 2005[1] requires each agency's Inspector General to review the policies and procedures related to PII and conduct reviews at least every 2 years to ensure it is adequately protected.

Impact on the Taxpayer

The IRS processes and maintains PII for more than 130 million taxpayers who file their income tax returns with the IRS. While the IRS has accomplished several noteworthy actions to protect this information, managers and employees have not complied with established security procedures. As a result, PII is being unnecessarily exposed to unauthorized access and potential identity theft.

Synopsis

The American public and Congress have become increasingly concerned about the protection of PII and identity theft. This issue is a significant challenge for the IRS, considering nearly 100,000 employees and contractors have access to tax return information processed on

[1] Public Law 108-447, 118 Stat. 2268, 5 U.S.C. 522a.

approximately 240 computer systems and more than 1,500 databases. Some of those employees are required to take sensitive taxpayer information out of the office on laptop computers to carry out their audit and collection responsibilities, increasing the risk that information could be lost or stolen.

The IRS has taken several noteworthy actions to protect taxpayer data in its possession. For example, it has established a Security Services and Privacy Executive Steering Committee to serve as the primary governance body for all matters relating to security and privacy issues in the IRS. In addition, it has made steady progress each year in complying with the requirements of the Federal Information Security Management Act of 2002.[2] Of particular note is that nearly all employees and contractors receive annual security awareness training.

However, our reviews during Fiscal Years 2003 – 2007 have identified persistent computer security weaknesses that continue to jeopardize the security of PII. We continue to identify that employees are not aware of the security risks inherent in their positions. Employees did not sufficiently safeguard laptop computers and did not encrypt data on the computers. Employees have also shown they are susceptible to social engineering techniques that hackers could use to gain access to their systems, and they continue to ignore IRS policies on the use of email, which increases potential security vulnerabilities. Even employees with key security responsibilities continue to ignore standard security configurations, often for their own convenience.

Our audits have shown that managers provide employees access to systems and data they do not need. In many cases, managers are not aware of the access capabilities of their employees. A fundamental goal of the IRS' computer modernization activities has been to provide more information to employees to improve their effectiveness and efficiency. New systems being developed will have the capability to provide even more information to these employees, which could actually increase the risk that the privacy of taxpayer information will be violated. The IRS will have to be more diligent in limiting employee access to a need-to-know basis.

We have also found that technical controls in modernized systems and the security infrastructure are inadequate. Although industry guidance recommends that security controls be designed into new systems early in the development process, security has not been at the forefront when new systems are developed in the IRS. Waiting until systems are implemented to address security controls will most likely cost significantly more than if security controls had been considered during the development of the systems. We have also found that audit trails[3] for detecting inappropriate accesses to taxpayer information on modernized systems are not being reviewed and retained.

[2] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[3] An audit trail is a chronological record of activities that allow for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to PII.

It is clear that some IRS executives are not holding managers and employees accountable for carrying out their responsibilities and for ensuring managers and employees are aware of the security risks associated with their positions. For the IRS to make greater strides in improving computer security and protecting PII, managers and employees must be aware of the security risks inherent to their positions and consider security implications in their day-to-day activities. Executives must clearly communicate expectations that procedures will be followed and take appropriate actions when procedures are not followed.

Recommendations

Because we have already made recommendations related to the aforementioned issues in our prior audit reports and the IRS is taking actions to address these deficiencies, no additional recommendations were made. We will continue to monitor the IRS' overall strategy and ability to protect and secure PII in future security-related reviews, where we may evaluate and report on the completion and effectiveness of actions taken to address security deficiencies.

Response

The IRS agreed that, while progress is being made, more needs to be done to ensure the issue of privacy and security over PII is a fundamental and top priority. The IRS will continue to update its systems, processes, and training so employees are aware of the steps they must take to prevent taxpayer information from being compromised. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report. 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.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

Management Has Taken Actions to Improve the Privacy of Sensitive Data ..... Page 3

Managers and Employees Are Not Complying With Established Security Policies and Procedures ..... Page 4

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 18

Appendix II – Major Contributors to This Report ..... Page 19

Appendix III – Report Distribution List ..... Page 20

Appendix IV – List of Security-Related Audit Reports ..... Page 21

Appendix V – Management's Response to the Draft Report ..... Page 22

Abbreviations

IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service
PII	Personally Identifiable Information

Background

The American public and Congress have become increasingly concerned about the protection of personally identifiable information (PII)[1] and identity theft. The Social Security Administration reports identity theft is one of the fastest growing crimes in America and encourages every citizen to protect his or her Social Security Number. The Commerce Department estimates more than 50 million identities were compromised in 2005, and the Federal Trade Commission reported it receives about 20,000 contacts from consumers each week about identity theft.

Identity theft is widely reported as the largest and fastest growing crime in America. The Federal Trade Commission receives about 20,000 complaints or inquiries each week from consumers about identity theft.

Several recent security breaches in private industry have made newspaper headlines. One recent example of identity theft, which was widely reported in the news media on December 14, 2006, linked identity theft to illegal immigration. Federal agents from the Immigration and Customs Enforcement agency raided 6 meatpacking plants in 6 States and arrested 1,282 illegal workers for stealing the identities of American citizens. The investigation determined that illegal immigrants had obtained Social Security Numbers and other PII from a variety of document fraud rings and vendors.

Because the Federal Government maintains a large quantity of PII, its agencies could be prime targets for identity theft. The Internal Revenue Service (IRS) stores PII for more than 130 million individual taxpayers who file their income tax returns each year with the IRS. Each tax return includes the filer's name, address, Social Security Number, and other personal information. Approximately 30 percent of the returns also include the names and Social Security Numbers of at least one dependent. In addition, the IRS maintains PII on its employees and contractors. The IRS identified the security of its computer systems as a high priority in its *2005 – 2009 Strategic Plan* and designated security as a material weakness under the Federal Managers' Financial Integrity Act of 1982.[2]

The challenge to protect PII from unauthorized disclosure is related not only to the magnitude of the data but also the complexity of ever-changing technology and the number of computer systems the IRS operates. The IRS processes and maintains PII using more than 240 computer systems and 1,500 databases. Most of its approximately 100,000 employees and contractors

[1] PII includes any information about an individual maintained by an agency including, but not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, etc.
[2] 31 U.S.C. Sections 1105, 1113, 3512 (2000).

have access to at least some of these data on a daily basis. To compound the risk that information could be lost or stolen, some IRS employees must take PII outside of their offices on laptop computers to carryout their audit and collection responsibilities. The competing goals of protecting PII and achieving workplace efficiencies become even more difficult as technology evolves and becomes faster and more complex.

To reinforce requirements for agencies to secure PII, Congress passed the Consolidated Appropriations Act of 2005[3] on December 8, 2004. The Act requires Federal Government agencies to appoint a Chief Privacy Officer with the primary responsibility of privacy and data protection. The Chief Privacy Officer is required to establish comprehensive policies and procedures and test the procedures to ensure they are followed. The Act also requires each agency's Inspector General to review the policies and procedures related to PII and conduct reviews at least every 2 years to ensure it is adequately protected.

This review was performed in the office of the Chief, Mission Assurance and Security Services, at the IRS National Headquarters in Washington, D.C., during the period December 2006 through March 2007. This review relied on audit results from Treasury Inspector General for Tax Administration security-related reports issued during Fiscal Years 2003 – 2007. The audits referenced in this report were conducted in accordance with *Government Auditing Standards* and are listed in Appendix IV. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[3] Public Law 108-447, 118 Stat. 2268, 5 U.S.C. 522a.

Results of Review

Management Has Taken Actions to Improve the Privacy of Sensitive Data

IRS executives and managers have taken several actions to protect PII. A Security Services and Privacy Executive Steering Committee was established in June 2006 to serve as the primary governance body for all matters relating to security services and privacy planning. The Committee is chaired by the Chief, Mission Assurance and Security Services, and includes representatives from each of the IRS business units. Each member is responsible for collecting and reporting on all privacy and security areas of concern.

Another important action to create a strong security environment was taken by the IRS Commissioner on June 1, 2006, when he issued an email to IRS managers emphasizing the importance of safeguarding PII. The Commissioner instructed all managers to:

> *Remind every IRS employee and contractor of their responsibility to safeguard taxpayer, employee, and all other personally identifiable information . . . and ensure that your employees are familiar with the policies and procedures the IRS has enacted to avoid privacy breaches.*

The Commissioner has also continued his efforts to dispel the perception that security is solely the responsibility of the Mission Assurance and Security Services organization by reminding executives that all managers and employees are responsible for the security of PII.

The importance of protecting PII will be emphasized in a video scheduled for distribution to IRS employees in the third quarter of Fiscal Year 2007. The video will include statements by the IRS Commissioner and the Treasury Inspector General for Tax Administration. One such statement made in the video will be, ". . . it is vital that every employee remain sensitive and vigilant to their commitment and responsibility to protect government equipment and PII." We believe these high-level actions from the top level of the organization send a strong message to all employees and are critical in transforming the IRS into a security-conscious organization.

The IRS has also made steady progress in recent years to comply with the Federal Information Security Management Act of 2002.[4] For Fiscal Year 2006, the IRS reported its computer

[4] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

systems had a certification and accreditation[5] rate of 95 percent, which is an improvement over Fiscal Year 2005 when only 35 percent of the systems were certified and accredited. During Fiscal Year 2006, the IRS reassessed the security risks of its computer systems, and we are confident that the inventory is substantially complete and the risk categorizations of the computer systems are accurate. The IRS also provided annual security awareness training to nearly all of its employees and contractors.

The IRS satisfied a major requirement of the Consolidated Appropriations Act of 2005 by appointing a Chief Privacy Officer to assume responsibility for privacy and data protection policies. The Chief Privacy Officer completed a comprehensive assessment[6] of the IRS privacy and data protection procedures and made recommendations to strengthen the controls.

The IRS also established an Identity Theft Program Office to identify security threats to itself and taxpayers and to develop approaches to best protect against the threats. To fulfill its responsibilities, the Identity Theft Program Office contracted with Deloitte Consulting to perform an identity theft risk assessment. The assessment, completed October 16, 2006, identified 113 business processes containing taxpayer information and characterized 48 of those processes as high priority from a risk perspective. IRS management selected 36 of the high-priority processes for indepth reviews.

Managers and Employees Are Not Complying With Established Security Policies and Procedures

While progress is being made, our prior reviews have identified persistent issues that continue to place the privacy and security of PII at risk. It is clear that some IRS executives are not holding managers and employees accountable for carrying out their responsibilities and are not ensuring managers and employees are aware of the security risks associated with their positions. For the IRS to make greater strides in improving computer security and protecting PII, managers and employees must be aware of the security risks inherent to their positions and consider security implications in their day-to-day activities. Executives must clearly communicate expectations that procedures will be followed and take appropriate actions when procedures are not followed.

The remainder of this report highlights some of the most significant security and privacy issues we have previously reported.

[5] Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of an accreditation, to determine the extent to which the controls are implemented correctly and operating as intended. Accreditation is the official management decision given by the owner of the information system to authorize the operation of the system and to explicitly accept the risks.
[6] *Policy and Process Review – Protection of Personally Identifiable Information (PII)*, dated June 26, 2006.

Employees did not safeguard laptop computers[7]

The IRS lost at least 490 computers and other sensitive data from 387 separate incidents between January 2, 2003, and June 13, 2006. For the 387 incidents, we determined it was unlikely that 176 incidents involved taxpayer data. For the remaining 211 incidents, we analyzed the incident writeups as of June 2006 and found 126 incidents 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 identity of taxpayers whose information may have been lost for the other 85 incidents due to a lack of detail in the incident writeups.

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

Employee negligence contributed to some of the losses. For example, 111 incidents occurred within IRS facilities, indicating 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, in the front seat or back seat of their vehicles, or 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 as luggage 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, could have been prevented if employees had taken more care to safeguard the computers.

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

[7] *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).

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.

We recommended the Chief, Mission Assurance and Security Services:

1. 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.
2. 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 IRS agreed with our finding and recommendations. The IRS also informed us that it has taken the following additional actions to address the loss of PII:

- Established a policy to notify individuals of the loss of their PII.
- Defined roles and responsibilities in the IRS' incident management process.
- Created a PII Incident Risk Analysis Methodology that it will use to categorize incidents and determine the appropriate IRS response.
- Created a PII Incident Notification Letter, which will be used to notify individuals whose PII has been compromised.

Employees were not encrypting PII on their laptop computers and other electronic media[8]

We selected 100 laptop computers from 4 IRS offices that support the Wage and Investment, Small Business/Self-Employed, and Large and Midsize Business Divisions and found that 44 of the 100 laptop computers contained unencrypted PII data such as:

- Individual Income Tax Returns (Form 1040).
- U.S. Corporation Income Tax Returns (Form 1120).
- Audit-related information, such as case history on current audits and financial data of taxpayers being audited.
- Various IRS forms with Social Security Numbers.

[8] *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).

- Employee evaluations, timesheets, and applications for reassignment.

In addition to the lack of encryption of PII on laptop computers, we found other computer devices on which PII was not always encrypted. Of the 100 employees in our sample, we found 54 were using various other electronic devices such as floppy disks, CDs, and DVDs to store unencrypted PII. Employees were using unencrypted CDs to backup taxpayer case information, to store grand jury information,[9] and to retain other PII provided by taxpayers.

The Office of Management and Budget requires agencies to ensure PII is encrypted on laptop computers and other electronic devices. To help employees encrypt the data, the IRS provided two encryption tools. First, laptop computers were configured to encrypt PII residing in specific file folders on the laptop computer's internal hard drive. This encryption tool is part of the computer's operating system. Employees need only save PII to these folders and the computer will automatically encrypt the data. The second encryption tool provided by IRS management is the WinZip software program, which is particularly useful when encrypting files not stored on the computers' internal drive, such as CDs and DVDs.

Despite the availability of the encryption tools, employees frequently chose not to encrypt PII. The employees placed the PII outside of the designated file folders for their own convenience or because they were unaware of the requirement to place the PII into the file folders. Some employees did not know their personal data were considered PII.

By not encrypting PII on laptop computers and other electronic devices, the IRS is needlessly exposing the data to unauthorized access, theft, or loss.

We recommended the Chief Information Officer:

1. 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.
2. 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.
3. 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.

[9] Grand jury information is all matters occurring before the grand jury. The grand jury is a jury of 12 to 23 persons convening in private sessions to evaluate accusations against persons charged with a crime and to determine whether the evidence warrants a bill of indictment.

The IRS agreed with our finding and recommendations. On March 5, 2007, the IRS informed us it had implemented a systemic disk encryption solution on laptop computers. This solution is intended to encrypt the entire hard drive of the laptop computer and requires access authentication, via login and password, whenever the laptop has been turned off. If the laptop computer is lost or stolen, unauthorized users would likely be unable to access any data on the hard drive.

Employees continue to be susceptible to social engineering attempts[10]

We were able to convince 61 managers and employees to give us their usernames and to change their passwords to one that we suggested. We conducted this review by calling 102 managers and employees and posing as computer support helpdesk personnel seeking assistance to correct a network problem. This common hacker tactic is referred to as social engineering, which involves exploiting the human aspect of computer security for the purpose of gaining insider information about an organization's computer resources.

The IRS' computer security procedures require employees to protect their usernames and passwords. Managers and employees must acknowledge the computer security rules prior to obtaining access to any IRS computer systems and annually recertify they are aware of their responsibilities. In addition, the IRS has posted these requirements and password security rules on its internal web site. The web site also has a document describing social engineering and providing examples of social engineering attempts, specifically mentioning the use of telephone calls to conduct social engineering attacks. While these awareness efforts are notable, our tests continue to show that some managers and employees still do not understand the rudimentary computer security practices of protecting their passwords.

The above conditions were particularly alarming because we had conducted similar social engineering test telephone calls in August 2001 and December 2004. Our August 2001 and December 2004 test calls yielded a 71 percent and 35 percent noncompliance rate, respectively. In response to these two prior audits, the IRS took corrective actions to raise awareness over password protection requirements and social engineering attempts. However, the corrective actions have not been effective. Based on the results of this audit, we concluded employees either do not fully understand security requirements for password protection or do not place a sufficiently high priority on protecting taxpayer data in their day-to-day work. In an attempt to better understand employee behavior, we asked the employees in our sample why they did not comply with guidelines for protecting their passwords. Some of the notable reasons given were that they thought the scenario sounded legitimate and believable, did not think that changing their password was the same as disclosing their password, or had experienced past computer problems.

[10] *Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers* (Reference Number 2007-20-107, dated July 20, 2007).

When employees are susceptible to social engineering attempts, the IRS is at risk of providing unauthorized persons access to computer resources and taxpayer data. With an employee's username and password, a hacker could gain access to PII on IRS computer systems. The hacker would gain the same access privilege as the employee. Even more significant, a disgruntled employee could use the same social engineering tactics to obtain another employee's username and password. With insider knowledge of IRS systems and applications, the disgruntled employee could more easily gain unauthorized access to IRS data as well as disrupt computer operations.

We recommended the Chief, Mission Assurance and Security Services, continue security awareness activities to remind employees of the potential social engineering attempts, conduct internal social engineering tests on a periodic basis to increase employee awareness of the need to protect usernames and passwords, and coordinate with business units to emphasize the need to discipline employees for security violations resulting from negligence or carelessness.

The IRS agreed with our findings and recommendations.

Employees were not following the IRS email use policy[11]

To determine whether IRS employees were complying with the IRS' personal use policy, we selected a statistical sample of 96 employees from its list of email addresses and reviewed 46,551 emails received and sent by these employees during June through August 2005. We found 2,576 messages in 71 (74 percent) of the 96 employee mailboxes that violated the IRS' personal use policy. These employees had from 1 to 288 inappropriate emails in their mailboxes. Specifically, we found the following types of inappropriate emails:

- Chain letters, jokes, and/or pictures accounted for 76 percent of the inappropriate emails. The content is often considered harmless on its own; however, it is well known that these messages present a security threat by being common carriers of malicious software.[12]
- Emails containing content considered offensive according to IRS guidelines accounted for 20 percent of the inappropriate emails. These emails contained hate speech and material that ridiculed others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Emails containing sexually oriented content, prohibited activities, and/or large files accounted for the remaining 4 percent of the inappropriate messages. Prohibited activities include activities conducted for commercial purposes, in support of for-profit activities, or in support of other outside employment.

[11] *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks* (Reference Number 2006-20-110, dated July 31, 2006).
[12] Malicious software is designed to infiltrate or damage a computer system, without the owner's consent. It includes computer viruses, spyware, and adware.

Figure 1 summarizes these email policy violations by type.

Figure 1: Email Policy Violations by Type

Chain Letters	1,953
Offensive Content	528
Sexually Oriented Content	55
Prohibited Activities	22
Large Files (graphics, video, sound, etc.)	18
TOTAL	**2,576**

Source: Our analysis of a sample of 96 IRS employees' email messages.

In May 2002, the IRS implemented a limited personal use policy for the Internet, email, and other equipment and resources.[13] The policy cautions employees to conduct themselves professionally and to refrain from using Federal Government information technology equipment for activities that are inappropriate based on established standards of conduct. The IRS considers email as inappropriate if it contains large, nonbusiness file attachments; chain letters; jokes; material that is offensive to other employees; or sexually oriented material. Email pertaining to illegal activities and other outside activities, such as running a business, fundraising, or restricted political activity, is also considered inappropriate.

We believe the high number of email policy violations occurred because the IRS has not effectively monitored the email of its employees to ensure compliance with the policy and has taken relatively few disciplinary actions on those employees who violate the policy. Between Fiscal Years 2003 and 2005, the IRS disciplined only 283 employees for abuse of email privileges. Of the 283 employees, 193 received written or oral counseling; 86 received formal disciplinary actions including admonishments, reprimands, suspensions, and removal; and 4 resigned. One additional case was referred to the Treasury Inspector General for Tax Administration Office of Investigations.

The large number of inappropriate emails places the IRS network at risk. For example, malicious software could be attached to these emails that could destroy data on the computer, enable unauthorized persons to access PII, and/or disrupt computer operations by causing a denial of service attack.[14]

[13] *IRS Policy on Limited Personal Use of Government Information Technology Equipment/Resources.*
[14] A denial of service attack inundates a computer system or network with traffic that overloads the system resources, causing them to cease operations or lose network connectivity.

In addition to the security risks, the performance and efficiency of the IRS' computing network is degraded by the number and size of inappropriate email messages. Many of the sampled messages contained graphics, sound, video, and/or animations that significantly increased the sizes of the files. Inclusion of these unnecessary features in an email message often increases a message's size from 10 times to 50 times the size of a normal text message, causing the system to operate slower and less efficiently, and creates the need for additional storage capacity that can be costly.

Offensive and inappropriate content in messages can also damage employee relationships and lead to adverse personnel actions or potential lawsuits. When forwarded to outside recipients, these messages could also invite high-profile media attention, thus damaging the IRS' reputation.

We recommended the Chief, Mission Assurance and Security Services:

1. Continue to emphasize the risks associated with inappropriate email use. If reminders that disciplinary actions have been taken against employees for email abuse are added to existing security awareness training, the number of violations may be reduced.
2. Consider implementing a program of monitoring email message content, which could subsequently increase the number of employees disciplined for abusing their email privileges. This approach will require a commitment of additional resources. However, considering the risks of subjecting the IRS network to malicious software, we believe this commitment is necessary.

The IRS agreed with our findings and recommendations.

Managers gave employees access to systems they did not need[15]

In an audit covering five systems in several IRS offices, managers and system administrators did not ensure user accounts for employees were removed from systems when employees left the IRS, transferred to another function, or changed job responsibilities. We identified 139 (21 percent) of 652 employees with active user accounts who, according to their managers, no longer had a business need to have system access. Keeping unneeded user accounts active increased the risk that unauthorized users could gain access to taxpayer data.

For the 513 employees who had a need to access the systems, we found no documentation that 128 (25 percent) had been properly authorized. Without the documentation, it was impossible to determine how these employees obtained access to the systems. We believe either managers did not carry out their responsibilities for formally approving employees' access or system administrators may have added employees to systems without a manager's authorization. When

[15] *Managers and System Administrators Need to Limit Employees' Access to Computer Systems* (Reference Number 2005-20-097, dated July 2005).

these employees leave the IRS or no longer need access to a system, their managers may not know they had access and the accounts will remain active.

A fundamental goal of the IRS' computer modernization activities has been to provide more information to employees to improve their effectiveness and efficiency. New systems being developed will have the capability to provide even more information to these employees, which could actually increase the risk that the privacy of taxpayer information will be violated. The IRS will have to be more diligent in limiting employee access to a need-to-know basis.

We recommended the Chief Information Officer:

- Enforce current procedures by configuring systems to automatically disable employees' accounts after 45 days of inactivity and to automatically delete the accounts after 90 days of inactivity.

We also recommended the Chief, Mission Assurance and Security Services:

- Coordinate with the business units to include tests of access controls during annual self-assessments required by the Federal Information Security Management Act. These reviews should reinforce to business unit managers the need to limit access to systems.

The IRS agreed with our findings and recommendations.

Managers were not consistently reviewing audit trail[16] information to identify unauthorized accesses to taxpayer accounts[17]

We determined a majority of IRS managers were not investigating potential unauthorized accesses to the Integrated Data Retrieval System (IDRS).[18] The IDRS is a mission critical system that contains PII such as taxpayers' names, Social Security Numbers, birth dates, addresses, and income. As stated earlier, the IRS operates about 240 computer systems that process PII. The IDRS is one such computer system on which audit trails are maintained and reviewed for questionable accesses.

IRS business unit managers must review and certify the following four IDRS Security Reports using the IDRS Online Reports Services system:[19]

[16] An audit trail is a chronological record of activities that allow for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to PII.
[17] *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 24, 2006).
[18] IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[19] This system is a web-based application that provides business unit managers and data security staffs online access to security reports based on the IDRS audit trail information.

- ***Sensitive Access Report*** – Issued weekly; identifies IRS employees who have accessed another employee's or an employee's spouse's tax accounts. The IRS requires business unit managers to determine whether employees made these accesses for work-related reasons. Business unit managers must take appropriate steps, including research on the IDRS and review of case assignment files, to identify the employees' reasons for the accesses. If needed, business unit managers may also interview the employees.
- ***Security Violations Report*** – Issued weekly; identifies unsuccessful logon attempts and employees who left their computers without logging off. Business unit managers should discuss these violations with their employees to determine whether unauthorized persons were trying to guess their passwords and whether the employees need additional training on using the IDRS.
- ***IDRS Security Profile Reports (2 reports)*** – Issued monthly and quarterly; identifies employees' capabilities on the IDRS and attempted accesses to taxpayer accounts using unauthorized command codes. Business unit managers should review these reports to ensure employees only have the access capabilities they need to perform their responsibilities and to determine whether all attempted accesses to taxpayer accounts using unauthorized command codes were unintentional errors.

IRS procedures require managers to review and certify the weekly IDRS Security Reports within 14 calendar days of receipt and the monthly and quarterly Security Profile Reports within 28 calendar days of receipt. For September 2005, we determined only 42 percent of IRS managers certified their IDRS Security Reports. Only 36 percent of these certifications were performed timely.

The Mission Assurance and Security Services organization and IRS business units have not sufficiently emphasized the need for business unit managers to review IDRS security reports and have not held their managers accountable for reviewing these reports on a regular basis. Without these reviews, the IRS cannot detect unauthorized accesses to PII. Employees may be browsing their neighbors' or other employees' tax accounts with little chance of detection.

We recommended the Chief, Mission Assurance and Security Services:

- Coordinate with IRS business units and place emphasis on the review of electronic IDRS Security Reports using the IDRS Online Reports Services system. Periodic compliance reviews should be conducted to ensure business units carry out their responsibilities to review IDRS Security Reports.

We also recommended the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement:

- Ensure all business unit managers' operational review requirements are updated to include a step to validate that all IDRS Online Reports Services system-related reports

are certified timely (by the manager or designee) and to hold the business unit managers accountable for meeting their security-related responsibilities.

The IRS agreed with our findings and recommendations.

Key security employees were not following security procedures, which allowed the IRS network system to remain vulnerable to insider attacks[20]

Our reviews of the IRS internal network system have identified persistent security weaknesses. In June 2005, we contracted with a computer security company to provide an objective internal network security review. This internal penetration test of the IRS network system identified six high-risk vulnerabilities that could allow an unauthorized person to gain access to PII. The following three vulnerabilities are well-known in the hacker community and related to incorrect or incomplete installation of software applications:

- Blank passwords to system administrator accounts on a database application were not changed. When the database application is installed, it contains a system administrator user account with a blank password. The database application vendor instructions and IRS installation procedures require changing the password to one that meets the IRS standard password configuration.
- Default logons and passwords on another database application were not changed. When the database application is installed, it contains default logons and passwords that are readily available from the Internet. The vendor's instructions and IRS installation procedures require changing or removing the default logons and passwords.
- Unneeded services were not removed, and security features such as patches[21] were not installed or updated. The operating system vulnerability, known as *sadmind*, is caused by not removing unneeded services and not adding security features patches. This vulnerability can be used to gain control of the host machine.

These three vulnerabilities were also identified and reported in our 2004 Penetration Test report and two of the three were reported in our 2003 Penetration Test report.[22]

IRS procedures provide adequate guidance to system and database administrators that, if followed, would have eliminated the above vulnerabilities. However, the vulnerabilities

[20] *Internal Penetration Test of the Internal Revenue Service's Networked Computer Systems* (Reference Number 2005-20-144, dated September 2005).
[21] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.
[22] *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2004-20-073, dated April 2004) and *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003).

persisted because system administrators chose to ignore controls for their own convenience and were not held accountable for complying with procedures.

When key security employees such as system administrators and database administrators do not follow IRS procedures, security risks and vulnerabilities exist that could permit the loss of PII. The risk to the IRS network system is especially high because a significant number of employees and contractors have access to the network.

We recommended the Chief Information Officer:

1. Examine the IRS' internal network to identify and correct the three exploited vulnerabilities. Specifically, the Chief Information Officer should ensure blank passwords for system administrator accounts on the databases are changed, default logons and passwords are changed, and *sadmind* vulnerabilities on computers with UNIX operating systems are corrected.
2. Enforce accountability and increase the awareness of database administrators and system administrators regarding the correct installation procedures for software, particularly database software.

The IRS agreed with our findings and recommendations.

The IRS and its contractors were not integrating security controls into modernized computer systems[23]

We identified several security technical control weaknesses in five modernization systems and the security infrastructure we reviewed, many of which could have been addressed during the development phase[24] of the systems as recommended by industry experts. For example, audit trails were not functioning and disaster recovery plans were not considered for the modernized systems we reviewed. In addition, documentation for the modernization systems indicated a lack of emphasis on security controls because it provided only general or outdated descriptions of security requirements.

The Mission Assurance and Security Services organization, the Business Systems Modernization Office (now called the Applications Development organization), and the PRIME contractor[25] are

[23] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005). We judgmentally selected and reviewed the e-Services, Internet Refund Fact of Filing, Modernized e-File, Custodial Accounting Project, and Customer Account Data Engine modernization projects.

[24] The development phase of a computer modernization project includes the analysis, design, construction, and testing of the new computer system.

[25] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.

responsible for incorporating security controls into modernization systems. The Mission Assurance and Security Services organization is responsible for establishing security standards for all computer systems. The Business Systems Modernization Office is responsible for ensuring security controls are considered and integrated in modernization systems. For the systems we reviewed, the Business Systems Modernization Office contracted with the PRIME contractor to develop security controls in accordance with IRS standards.

The PRIME contractor focused on developing systems that would function but did not provide sufficient emphasis on the identification and development of security controls. In addition, the Mission Assurance and Security Services organization was not sufficiently involved during the early development stages of the systems. More involvement was needed to hold the PRIME contractor accountable and to encourage the contractor to develop adequate security controls when the systems were being developed.

Waiting until systems are implemented to address security controls will most likely cost significantly more than if security controls had been considered during the development of the systems.

We recommended the Chief Information Officer:

1. Provide oversight to ensure coordination between the Business Systems Modernization Office and its contractors. The Business Systems Modernization Office should retain the overall responsibility for ensuring security controls are provided in the development phase of new projects.
2. Revise the Enterprise Life Cycle[26] to require disaster recovery planning during the development phase. A complete Disaster Recovery Plan should be required that addresses all modernization systems. During development, computer capacity and business resumption requirements should be gathered and considered.
3. Ensure audit trail data captured for the Customer Account Data Engine[27] are retained and reviewed to detect unauthorized accesses.

The IRS agreed with the finding and the first two recommendations but disagreed with the third recommendation. The log and audit files used by the Customer Account Data Engine system programmers are established for recovery and diagnostic purposes and do not capture data related to unauthorized access. Currently, the Customer Account Data Engine has no support for external data inquiry.

[26] The Enterprise Life Cycle is the set of repeatable processes the IRS and its contractors follow to modernize the IRS' computer systems.
[27] The Customer Account Data Engine is an online modernization data infrastructure that will house taxpayer accounts and tax returns.

We continue to believe audit trail information for the Customer Account Data Engine should be retained and reviewed because it currently contains tax information for more than 1.3 million returns that could be accessed by some IRS employees for unauthorized purposes and potentially used for identity theft purposes. Accordingly, audit trail information must be maintained to comply with Department of the Treasury requirements.

We also recommended the Chief, Mission Assurance and Security Services:

4. Participate in the development phase of new systems and ensure security controls are built into the systems.

The IRS agreed with the recommendation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the progress the IRS has made in ensuring the security and privacy of PII it maintains. To accomplish our objective, we:

I. Summarized the progress the IRS has achieved in securing the privacy of PII.

A. Interviewed the Director of the IRS Office of Privacy and Information Protection to determine the progress achieved during Fiscal Years 2003 – 2007. We reviewed documentation provided by the Director of the Office of Privacy and Information Protection.

B. Reviewed the Treasury Inspector General for Tax Administration security-related audit reports issued during Fiscal Years 2003 – 2007 and identified the positive issues reported.

C. Reviewed the policy and process review entitled, "Protection of Personally Identifiable Information," that was completed by the IRS Chief Privacy Officer on June 26, 2006.

D. Reviewed the Identity Theft Risk Assessment report prepared by Deloitte Consulting on October 16, 2006.

II. Reviewed audit reports issued by the Treasury Inspector General for Tax Administration during Fiscal Years 2003 – 2007 to identify the most significant security-related weaknesses reported.

III. Identified the overall causes for the weaknesses identified in Step II.

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
Allen Gray, Lead Auditor
Myron Gulley, Senior Auditor

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Acting 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

Appendix IV

List of Security-Related Audit Reports

This report refers to the following security-related audit reports issued during Fiscal Years 2003 – 2007. The prior reports are listed in order of appearance in this report.

- *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).
- *Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers* (Reference Number 2007-20-107, dated July 20, 2007).
- *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks* (Reference Number 2006-20-110, dated July 31, 2006).
- *Managers and System Administrators Need to Limit Employees' Access to Computer Systems* (Reference Number 2005-20-097, dated July 2005).
- *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 24, 2006).
- *Internal Penetration Test of the Internal Revenue Service's Networked Computer Systems* (Reference Number 2005-20-144, dated September 2005).
- *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2004-20-073, dated April 2004).
- *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003).
- *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005).

Appendix V

Management's Response to the Draft Report

RECEIVED
JUL 2 0 2007

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

July 20, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel Galik D. Galik
Associate Chief Information Officer, Cybersecurity

SUBJECT: Draft Audit Report – Efforts Have Been Made, but Managers' and Employees' Noncompliance with Security Policies and Procedures Put Personally Identifiable Information at Risk (Audit #200620007) (i-trak #2007-25942)

Thank you for the opportunity to comment on the subject draft report that summarizes Treasury Inspector General for Tax Administration's (TIGTA) past audits issued during Fiscal Years 2003 to 2007, addressing the security and privacy of personally identifiable information (PII). The issue of privacy and security over PII is a fundamental and top priority for the IRS. We continue with vigilance to address the challenges and risks associated with protecting taxpayers PII processed and maintained on our computer systems.

We appreciate the fact that your report acknowledges that progress is being made, and we agree that more needs to be done. We continue to update our systems, processes, and training so that employees who have access to sensitive information are aware of the steps they must take to prevent taxpayer information from being compromised. Some of the recent security measures the IRS has implemented to enhance the protection of sensitive information are listed below:

- Installation of automatic full disk encryption solution on the total deployed inventory of 52,511 IRS laptops.
- Establishment of a Security Services and Privacy Executive Steering Committee to provide oversight over the initiatives and plans that are developed to strengthen the security and privacy posture of the IRS.
- Establishment of a new executive position, reporting directly to the IRS Deputy Commissioners, which will focus on taxpayer privacy and identity theft.
- Establishment of a new executive position, reporting directly to the Chief Information Officer, with responsibility for managing the IRS-wide IT security program to ensure

compliance with the requirements of the Federal Information Security Management Act (FISMA).

- Implementation of a comprehensive communications strategy to educate employees on asset and data protection responsibilities and the use of encryption capabilities.
- Deployment of mandatory information protection training for all employees and contractors with access to sensitive information.
- Implementation of a layered security "defense-in-depth" approach with the deployment of upgraded firewalls and intrusion detection devices, while maintaining a 24 X 7 cyber security incident response center (CSIRC) to monitor IRS computer and network security.
- Issuance of numerous updated data protection policies, processes, and education training tools to improve employee awareness and skill levels.

The privacy and security of both taxpayer and employee information is one of our highest priorities, and we look forward to working with TIGTA in the future on this important issue. If you have any questions, or if you would like to discuss this further, please contact me at (202) 622-8910.