TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

July 2001

Reference Number: 2001-20-108

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 | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 23, 2001

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

This report presents the results of our review of physical security at five Internal Revenue Service (IRS) facilities. In summary, we found security weaknesses that could allow an intruder easy access to IRS facilities and computer resources. Many of the weaknesses have persisted even though previously identified.

We recommended that the Chief, Agency-Wide Shared Services (AWSS), the Deputy Commissioner for Modernization & Chief Information Officer, and functional managers should coordinate efforts to improve employee security awareness. Management should provide the funds necessary to correct the specific security weaknesses we identified. The AWSS should also coordinate with the General Services Administration to ensure security weaknesses in multi-tenant buildings are corrected when identified.

Management agreed with our recommendations. However, regarding the control of equipment and data used in the Volunteer Income Tax Assistors program, they questioned the validity of the specific methods recommended. In those instances, we provided comments to clarify our position concerning the implementation of controls. Management's written response discusses several corrective actions that will improve the reported conditions. Their comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, “Limited Official Use Information and Other Legends” of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA’s Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions, or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

Table of Contents

Executive Summary

In recent months, certain federal agencies have incurred very damaging security breaches that can be traced to physical security weaknesses. These breaches may have caused the unauthorized disclosure of sensitive documents and data. Inadequate physical security could also lead to the loss of property and to the disruption of critical services.

With the emphasis on customer service, telecommunications advances, and the wide use of laptop computers, taxpayer data are much more accessible in the Internal Revenue Service (IRS) workplace. This new accessibility has also brought greater challenges for physically securing the data. While it is still more critical to provide physical security at major processing centers, employees (and intruders) can now access vast amounts of sensitive data at IRS offices and even small posts of duty.

We conducted this review to determine whether the IRS has adequate physical security controls to safeguard computer resources and data from the threat of misuse, loss, and damage. The Treasury Inspector General for Tax Administration and the General Accounting Office have conducted several physical security tests in recent audits. For this audit, we reviewed a computing center and four other offices to make our assessments.

Results

Over the past several years, IRS management has been implementing a strategic plan to methodically assess and improve physical security. As a result, security has been significantly improved at many IRS sites. In spite of these efforts, IRS facilities remain vulnerable to intruders, explosive attacks, theft of computer resources, and unauthorized disclosure of taxpayer data even in those offices where IRS has completed vulnerability assessments and improvements. Also, controls over laptop computers taken out of IRS facilities were weak.

The IRS has adequate policies and procedures for physical security. The procedures related to the issues in this report were not implemented, we believe, due to a lack of attention to security controls, insufficient security reviews, funding limitations, and ineffective coordination with the General Services Administration (GSA) at multi-tenant locations.

Controls Were Not Always Sufficient to Prevent Unauthorized Access to Buildings and Computer Resources

While we recognize the difficulty in preventing access to a determined, experienced intruder, the IRS could strengthen controls to prevent most unauthorized accesses. For example, there were numerous perimeter security vulnerabilities at various building entry points, including loading dock areas. Perimeter doors were left propped open, unlocked, or unguarded. Security gates were unlocked and perimeter fencing was in need of maintenance. And, several opportunities existed for bomb-laden vehicles to park near IRS facilities without detection. In addition, access cards and identification badges were not properly controlled increasing the risk they could be used to gain unauthorized access to IRS facilities.

Security of Laptop Computers Needs Improvement to Deter Theft and to Protect Taxpayer Data

Technology advances have enabled users to store large amounts of data on laptop computers. These computers enable users to take vast amounts of sensitive data outside the perimeter of IRS facilities and the confines of secure computer rooms. The portability of laptops greatly increases the risk that these computers could be lost or stolen. Based on poor inventory practices at the offices we visited, we could not determine if all laptops were accounted for. In addition, laptops were not properly secured after hours at one location.

Also, taxpayer information stored on approximately 5,000 laptops used by volunteer tax assistors was vulnerable to unauthorized disclosure. Systems used by these volunteers were not password protected, data were not encrypted, and taxpayer information was not removed from the hard drives of the laptops when no longer needed.

Summary of Recommendations

The Chief Agency-Wide Shared Services (AWSS) and functional managers should coordinate efforts to improve employee security awareness. Management should provide the funds necessary to correct the specific security weaknesses we identified. The AWSS should also coordinate with the GSA to ensure security weaknesses in multi-tenant buildings are corrected when identified. Management should develop procedures to ensure that volunteer tax assistors regularly remove taxpayer data from the hard drives of laptop computers and that the volunteers return the laptops to the IRS at the end of the filing season.

Management's Response: Management agreed with our findings and recommendations and provided specific actions aimed at increasing the security awareness of functional managers. The AWSS has implemented a Security Survey and Risk Assessment Program for all IRS facilities. This program should identify facility threats and weaknesses by applying a uniform risk assessment methodology to all facilities, and improve coordination with the GSA to resolve security vulnerabilities in multi-tenant buildings.

Management characterized our recommendations to assign accountability over laptop computers and taxpayer data used in the Volunteer Income Tax Assistor (VITA) program as not practical and not cost effective. The Director, Stakeholder Partnership, Education and Communication (SPEC), who is responsible for the VITA program, stated that SPEC territory managers are assigned the responsibility and accountability over laptops, and the Director is exploring methods of protecting data generated during the return filing process.

The Director indicated that returning the laptops to the IRS at the end of the filing season would not be practical and contravenes the Congressional mandate to increase the number of electronically filed returns. The Director further asserted that one of our recommendations would jeopardize the entire VITA program.

Office of Audit Comment: We agree with assigning accountability for VITA laptops to the SPEC territory managers. We also agree that SPEC managers should ensure that the VITA site coordinators reinforce the message to protect taxpayer data and government computers. However, the Director, SPEC, appears to be abdicating responsibility for safeguarding the laptops during the 8-month period between filing seasons. We believe the risk of theft or loss of taxpayer data and government equipment justifies the cost of controlling these assets. We also believe that the need to safeguard these assets does not contravene the Congressional mandate to increase the number of electronically filed returns.

In our opinion, management's assertion that our recommendation would jeopardize the VITA program is unreasonable. However, the alternatives management is exploring to protect taxpayer data on VITA laptop computers have merit. Our concern is that the implementation date for protecting taxpayer data on laptops is July 2002, meaning that the IRS will go through another filing season with the unnecessary risk of losing or compromising taxpayer data. In our opinion, corrective actions can and should be taken before January 2002.

Objective and Scope

Our overall objective was to evaluate physical security controls over computer resources and data.

Our overall objective was to determine whether the Internal Revenue Service (IRS) had effective physical security controls to safeguard computer resources and data from the threat of misuse, loss, and damage.

We evaluated the IRS' compliance with requirements and guidelines issued by the IRS, the U.S. General Accounting Office (GAO) and the National Institute of Standards and Technology. Our review of controls included observation, interviews with both Information Technology Services (ITS) and Agency-Wide Shared Services (AWSS) personnel, and testing exterior and interior entry controls.

We performed this audit between October 2000 and December 2000 at the Tennessee Computing Center, and the Dallas, Phoenix, and two Manhattan offices. The audit was performed in accordance with *Government Auditing Standards.*

At each of the sites we visited, we evaluated the security of the building's perimeter and entrances, the security environment inside the building, and access to the computer and telecommunications equipment rooms. Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Effective physical security controls are essential to protecting computer systems, data and personnel.

Physical security controls provide for the protection of property, personnel, computer systems, and data, against unauthorized access, damage, sabotage, or other illegal or criminal acts. Certain federal agencies have recently incurred very damaging security breaches that can be traced to physical security weaknesses. These breaches

may have led to the loss of property, the disruption of services and functions, and the unauthorized disclosure of sensitive documents and data.

With the emphasis on customer service, telecommunications advances, and the wide use of laptop computers, taxpayer data are much more accessible in the IRS workplace. This new accessibility has also brought greater challenges for physically securing the data.

Physical security controls at the IRS have been the subject of numerous reviews.

The Treasury Inspector General for Tax Administration (TIGTA), the GAO and the IRS Office of Security Evaluation and Oversight (SEO) have reported on IRS physical security controls. The TIGTA has, most recently, included this subject in overall security reviews at three former district offices,[1] and identified several weaknesses. The GAO has been reporting for several years on computer security at the IRS. The Office of SEO regularly conducts reviews to ensure that IRS offices are in compliance with physical security standards and requirements. The IRS is also in the process of conducting vulnerability assessments and security surveys at its facilities, many of which have been completed. For this audit, we chose locations to complement the prior audit work.

[1] *Computer Security Controls Should Be Strengthened in the Houston District*, (Reference Number 2000-20-106, dated July 2000); *Computer Security Controls Should Be Strengthened in the Former Brooklyn District*, (Reference Number 2001-20-020, dated November 2000); *Computer Security Controls Should Be Strengthened in the Former Northern California District*, (Reference Number 2001-20-036, dated January 2001).

Results

A lack of emphasis on physical security policies and procedures could allow intruders easy access to IRS facilities and computer resources.

IRS facilities remain vulnerable to intruders, explosive attacks, theft of computer resources, and unauthorized disclosure of taxpayer data. We identified several security weaknesses at the computing center and four other offices that could allow an intruder easy access to IRS facilities and computer resources. Specific examples of these conditions, where they were found, and the related causes are presented in Appendix IV. Also, data on laptop computers could be better protected from theft and unauthorized disclosure.

The IRS has adequate policies and procedures for physical security. The procedures related to the issues in this report were not implemented for several reasons. Security policies and procedures have long been emphasized at the computing centers to a greater extent than at smaller offices, because of the amount and type of data physically stored there. Although employees (and intruders) at the smaller offices now have access to the same data via telecommunications, security at these facilities has not been emphasized to the same degree.

We also attributed the weaknesses we identified at all sites to insufficient security reviews by on-site physical security personnel, a lack of funding allocated for security improvements, and the need for improved coordination with the General Services Administration (GSA) at multi-tenant locations. Many of the conditions we noted had been identified in prior reviews but had not been corrected.

Controls Were Not Always Sufficient to Prevent Unauthorized Access to Buildings and Computer Resources

The first line of defense in protecting a facility and the resources within from intruders and building attacks are

the security controls placed at the property line and building perimeter. While we recognize the difficulty in preventing access to a determined, experienced intruder, the IRS could strengthen controls to prevent most unauthorized accesses. We noted the following conditions.

Facilities were vulnerable to explosive attacks

The Consolidated Physical Security Standards for IRS Facilities (CPSS) provides a set of minimum physical security standards. The CPSS states that receptacles that could conceal explosives should be kept away from the building; passive vehicle barriers, such as security bollards, should be provided at all IRS facilities; and signs indicating the location of sensitive assets should be minimized.

We identified instances where:

Perimeter controls were not sufficient.

- Perimeter fencing at the computing center was not properly maintained.
- Vehicles were permitted to enter the computing center grounds and travel through the property to the loading dock before being inspected for explosives.
- Newspaper receptacles that could be used to conceal explosive devices were placed against an office building (see figure 1).

Figure 1: Receptacles placed against a building.

- Security gates and retractable bollards were not in place or in use to protect two of the four smaller offices against bomb laden vehicles (see figures 2 and 3).

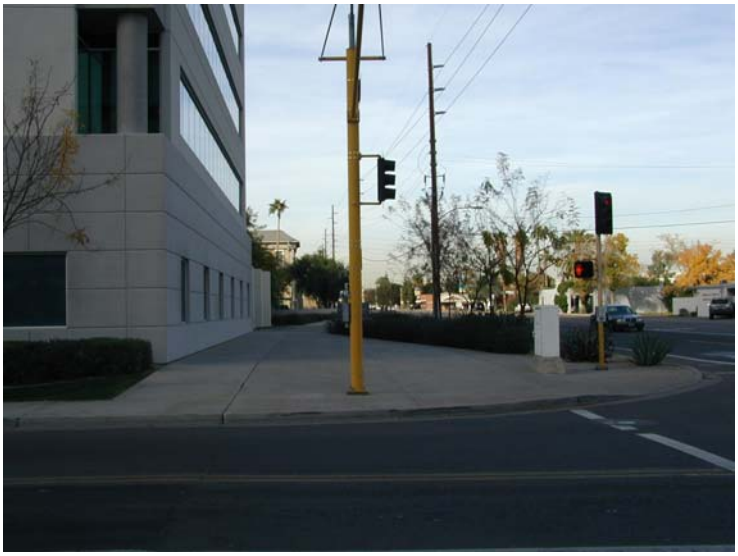

Figure 2: Stationary bollards not in place.

Figure 3: Gate open with bollards retracted.

- A shared driveway at one office could have been used for a bomb-laden vehicle to enter and park at an unguarded loading dock without detection (see figure 4).

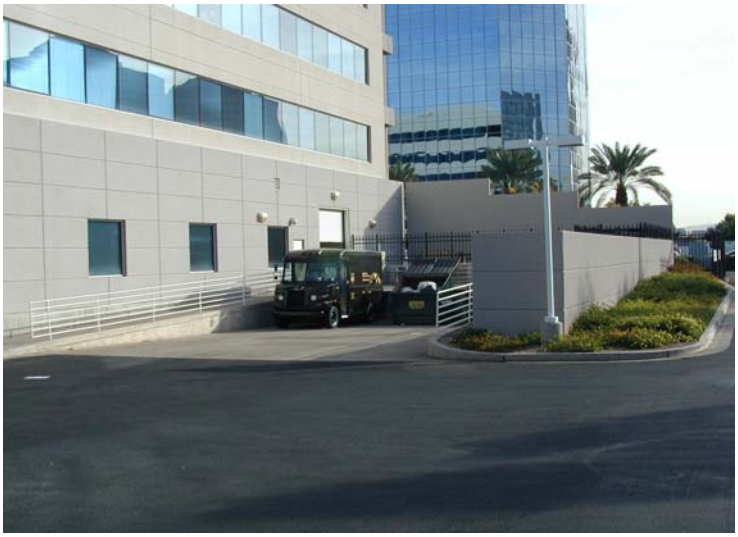

Figure 4: Unguarded loading dock at shared driveway.

- Signs outside the computing center and inside an office brought unnecessary attention to IRS facilities and computer resources (see figure 5).

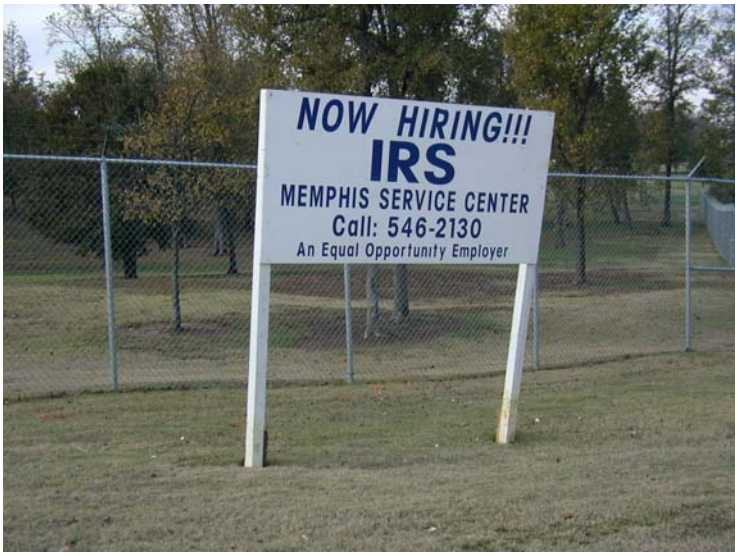

Figure 5: Sign identifying an IRS facility.

Management was aware of many of these conditions, but had not taken action either because of cost considerations, lack of awareness of the potential security risks, or lack of coordination with the GSA or other IRS management.

Perimeter doors were not adequately secured

The Department of the Treasury and IRS security standards require that all perimeter doors be locked and alarmed when not guarded. Management must conduct regular reviews of these controls to ensure they are functioning properly and must also train employees to be alert to security vulnerabilities.

Easy access to IRS facilities could be obtained through doors that were unlocked, propped open, not alarmed, or unguarded.

We identified instances where perimeter doors at two offices were unlocked, propped open, did not properly close, were either not alarmed or had an alarm that was not functioning, or were not properly guarded. These weaknesses could allow intruders, visitors, or employees to surreptitiously enter the buildings, or to remove data or computer resources without detection.

These conditions occurred because employees were not alert to security vulnerabilities, and the AWSS staff did not adequately review security controls to ensure that

locks and alarms were functioning properly. Also, the AWSS staff did not coordinate with the GSA to have an alarm installed on a fire exit door shared by all building tenants. Management cited a lack of funding as the cause of inadequate guard service at doors where needed.

Identification badges and keys were not adequately controlled

The IRS requires managers to ensure that employees wear their identification (ID) badges properly at all times. On a daily basis, the Security office should receive notification from the Personnel function to adjust the ID badge records of separating employees. Records of issuing offices must account for all ID badges, and inventory and destruction records should be maintained.

At two offices, many employees did not wear ID badges. We also noted insufficient controls, at a computing center and one other office, over electronic key cards and ID badges. A master key at one office was cut from a key form that could have been duplicated. These conditions could have made it easier for an intruder to gain unauthorized access to facilities and resources.

We attributed these conditions to a lack of attention to existing security procedures.

Computer facilities and data were not adequately secured

The Internal Revenue Manual (IRM) requires that controls be in place to safeguard computer resources. All visitors must be escorted while in computer and telecommunications equipment rooms and their visits must be recorded in access logs. In addition, inventory controls, including sign-out logs, must be in place to account for magnetic media, and backup media must be stored off-site.

At one office, access to the telecommunications equipment rooms was not sufficiently limited or monitored. Also, there was no inventory of stored magnetic media and no sign-out log for the tape library at this office. At another office, the inventory was inaccurate making it difficult to account for the media. Two offices did not have off-site storage for backup media.

These weaknesses were due to a lack of attention to existing security procedures and insufficient emphasis on security of magnetic media storage.

Recommendations

We recommend that the Chief, AWSS:

1. Coordinate with functional managers to place additional emphasis on employee awareness of physical security controls such as the importance of wearing ID badges and being alert to open or unlocked doors and gates and other conditions that place the employees and facilities at risk.
2. Place alarms on fire exit doors to discourage employees from opening the doors in non-emergencies and leaving them unsecured.
3. Ensure that local AWSS staff regularly evaluate and maintain security controls to ensure they are in place and functioning properly.
4. Allocate funding to increase guard service, and to implement security controls such as magnetometer and X-ray machines where needed.
5. Ensure that local AWSS management coordinates with the GSA where necessary. While the GSA is responsible for correcting physical security weaknesses in buildings housing multiple agencies, the AWSS should identify weaknesses and follow up with the GSA to ensure improvements are made.

Management's Response: The AWSS will coordinate with IRS managers, in those instances where the security weaknesses are within the IRS' control, by ensuring that all employees understand IRS security policies and by assisting managers in fulfilling their obligation through security awareness training. In those instances where the vulnerability is outside of IRS controlled space, the AWSS will coordinate with the applicable primary authority (the GSA, the Federal Protective Service, and/or through a Building Security Committee) to resolve the identified weaknesses. The AWSS has implemented a Security Survey and Risk Assessment Program for all IRS facilities. This program should identify facility threats and weaknesses by applying a uniform risk assessment methodology to all facilities, and improve coordination to resolve security vulnerabilities in multi-tenant buildings.

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer:

6. Ensure that local ITS management review access to the telecommunication equipment rooms and ensure access is limited based on need, and that visitors sign an access register and are monitored while in the room.
7. Ensure that management at IRS offices remove any signage that draws unnecessary attention to IRS facilities and computer resources.
8. Improve controls to ensure that magnetic media is accounted for and backup tapes are stored off-site.

Management's Response: The Director, Information Technology Systems Field Operations, will issue guidelines to ITS managers to enforce security requirements for access to telecommunication equipment rooms, for proper maintenance of magnetic media inventory, and for off-site storage of backup tapes. Also, the Office of Security will work with Computing Center Directors and other office heads to

remove signage that draws unnecessary attention to an IRS facility and computer resources.

Security of Laptop Computers Needs Improvement to Deter Theft and to Protect Taxpayer Data

Technology advances have enabled users to store large amounts of data on laptop computers. The portability of these computers enables users to take the laptops and sensitive data outside the perimeter of IRS facilities and the confines of secure computer rooms, greatly increasing the risk that sensitive data could be lost or stolen. Their portability and value also make laptop computers prime targets for theft.

The Office of Management and Budget requires that each agency establish and maintain control of computer inventories to avoid fraud, waste and abuse. However, management must rely upon employees to provide adequate physical security over laptops both on-site and when they are removed from IRS premises.

Physical security of laptops provided to employees was not adequate

At least five laptop computers were lost or stolen, during Fiscal Year 2000, from one office we reviewed.

ITS management at one office determined that five laptop computers could not be located during a recent physical inventory of computer equipment. However, the number of lost or stolen laptops could be even higher. Due to poor inventory practices at three offices, we could not determine if any additional laptops were missing.

At one office, 21 laptop computers were not secured during non-duty hours, in violation of IRM requirements for securing portable computers. Weaknesses in perimeter security at this site increased the risk that unsecured laptops could be easily stolen and removed from the premises without detection. These conditions

occurred because employees did not provide sufficient effort in securing laptop computers.

Taxpayer data on laptop computers provided to volunteer tax assistors was not safeguarded

Taxpayer data on more than 5,000 laptop computers used by volunteer tax assistors was not protected from loss or unauthorized disclosure.

During the 2001 filing season, more than 5,000 IRS laptop computers were used by volunteers who were, for the most part, not IRS employees. These volunteers prepared and stored approximately 440,000 tax returns on laptop computers. The risk of theft is greater for these computers since the IRS cannot ensure that the laptops are physically secured while in the possession of the volunteers.

Taxpayer data stored on these laptops was particularly vulnerable because:

- Data were not encrypted. Department of the Treasury policy states that encryption of electronically stored sensitive information on portable computing devices, such as laptop computers, is mandatory.
- The Windows 98 operating system used on the laptops was not password protected.
- Password protection options available with the software used to prepare tax returns did not prevent an unauthorized user from viewing taxpayers' return information saved to the laptop hard drive.
- The IRS did not require that tax return information stored on the laptops be removed as soon as the electronically filed returns are accepted and the data were no longer needed by the volunteers. Also, a disk wiping utility was not provided to the volunteers to remove taxpayer data before returning the laptops to the IRS at the end of the filing season. At one location, we found taxpayer information remained on the laptop computers nearly 1 year after the volunteers returned the laptops to the IRS.

- Two of the offices reviewed did not provide volunteers with information on protecting taxpayer data. Department of the Treasury policy also requires that users of laptops processing sensitive information must sign a responsibility statement which stipulates that they understand the security measures necessary to protect that information.

Taxpayer data provided to volunteers was not adequately secured because the IRS has determined that it is not legally responsible for protecting the taxpayer information provided to the volunteer tax assistors. While the IRS may not be legally responsible, it could be subject to negative publicity if sensitive taxpayer data were lost, stolen, or improperly disclosed.

Recommendations

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer:

9. Periodically remind employees (for example, through Leave and Earnings Statement flyers) of the proper storing and securing of laptop computers on IRS premises.

10. Assign accountability over laptops given to volunteer tax assistors to an IRS employee in each office. Develop procedures to ensure that all laptops issued to volunteer tax assistors are returned to the IRS at the end of the filing season.

11. Establish procedures, in conjunction with the Director, Stakeholder Partnership, Education and Communications, to regularly remove taxpayer data from the hard drives of laptop computers used by volunteer tax assistors, and follow up with the assistors to ensure compliance.

Management's Response: Action will be taken to periodically remind employees about the proper storage and securing of laptop computers via various

communications, including flyers in Leave and Earnings Statements.

Management characterized our recommendations to assign accountability over laptop computers and taxpayer data used in the Volunteer Income Tax Assistor (VITA) program as not practical and not cost effective. The Director, Stakeholder Partnership, Education and Communication (SPEC), who is responsible for the VITA program, stated that SPEC territory managers are assigned the responsibility and accountability over laptops, and the Director is exploring methods of protecting data generated during the return filing process. The Director indicated that returning the laptops to the IRS at the end of the filing season would not be practical and contravenes the Congressional mandate to increase the number of electronically filed returns. The Director further asserted that one of our recommendations would jeopardize the entire VITA program.

Office of Audit Comment: We agree with assigning accountability for VITA laptops to the SPEC territory managers. We also agree that SPEC managers should ensure that the VITA site coordinators reinforce the message to protect taxpayer data and government computers. However, the Director, SPEC, appears to be abdicating responsibility for safeguarding the laptops during the 8-month period between filing seasons. We believe the risk of theft or loss of taxpayer data and government equipment justifies the cost of controlling these assets. We also believe that the need to safeguard these assets does not contravene the Congressional mandate to increase the number of electronically filed returns.

The Director, SPEC, stated that the recommendation to remove taxpayer data from the hard drives of laptops used by assistors, as it stands, would jeopardize the entire VITA program. In our opinion, management's assertion that our recommendation would jeopardize the

VITA program is unreasonable. However, the alternatives management is exploring to protect taxpayer data on VITA laptop computers have merit. Our concern is that the implementation date for protecting taxpayer data on laptops is July 2002, meaning that the IRS will go through another filing season with the unnecessary risk of losing or compromising taxpayer data. In our opinion, corrective actions can and should be taken before January 2002.

Conclusion

The risks of explosive attacks, theft of IRS resources, and unauthorized disclosure of data have increased in recent years; and, so has the difficulty in preventing such attacks and intrusions. Increased funding, more reviews, and improved coordination with the GSA will help diminish these risks. But, the biggest hurdle will be to educate managers and employees in all offices of the risks so that they can make physical security part of their daily routines.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) had effective physical security controls to safeguard computer resources and data from the threat of misuse, loss, and damage. To accomplish our objective, we performed the following audit tests at the Tennessee Computing Center, and the Dallas, Phoenix, Midtown Manhattan, and Downtown Manhattan offices.

I. Observed and evaluated physical security safeguards at building and facility perimeters used to deter and detect intruders and building attacks.

   A. Observed building and facility perimeter security including: perimeter fences and gates, surveillance systems, loading dock areas, parking garages, ground floor windows, secured entry points, public parking areas, main utility feeds, etc.

   B. Interviewed Security Office personnel to identify policies and procedures for restricting entrance to IRS buildings and individual floors. Observed building entry points and access to floors to assess compliance with policies and procedures for controlling access and screening employees and visitors (i.e., visitor log, use of visitor and employee identification badges, use of X-ray and magnetometer, etc.).

II. Observed and evaluated security controls inside the building for limiting access to computer resources to only authorized individuals.

   A. Determined if computer rooms and telecommunication equipment rooms were maintained under a low profile.

   B. Evaluated controls over access to the computer room at the Tennessee Computing Center, and the IRS office telecommunications equipment rooms.

   C. Evaluated controls over deposits and withdrawals of tapes and storage media at the tape library.

   D. Conducted an after-hours security check to observe controls for limiting access to computer resources.

III. Identified and evaluated controls to protect laptop computers and the sensitive data stored on the laptops, if any.

A. Interviewed Agency-Wide Shared Services and Information Technology Services personnel to identify policies and procedures to limit access and safeguard laptop computers from theft or loss.

B. Conferred with the building Security Office to determine whether building security breaches and thefts or loss of laptop computers have been reported. Analyzed the probable causes for the security breaches and thefts or loss of laptops.

C. For any lost or stolen laptop computers, determined if sensitive data was stored on hard drives or some exterior storage device (i.e., floppy disks).

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Bret Hunter, Senior Auditor
Joan Raniolo, Senior Auditor
Charles Ekholm, Auditor
David Hodge, Auditor
James McCormick, Auditor
William Simmons, Auditor
Theodore Tomko, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Chief Financial Officer, Department of the Treasury
Chief, Agency-Wide Shared Services A
Director, Office of Security M:S
Director, Security, Evaluation and Oversight M:S:S

Appendix IV

Examples of Security Vulnerabilities

Facilities were vulnerable to explosive attacks

- Large gaps under the perimeter fence at the Tennessee Computing Center (TCC) could have allowed an intruder to enter the facility grounds. Building operations personnel had not kept up with the maintenance of the fence.
- Vehicles were permitted to enter the grounds of the TCC and travel through the property to the loading dock before being inspected for explosives. Management was aware of this vulnerability but stated that the cost to reconfigure the facility entrance to accommodate truck inspections would be prohibitive.
- Many newspaper receptacles that could be used to conceal explosive devices were placed against two walls of the building housing the Dallas office. Management was aware of this condition but did not effectively coordinate with the General Services Administration (GSA) to ensure the hazard was removed. GSA personnel stated they had planned to remove the receptacles for aesthetic reasons but were not aware they posed a security risk.
- Devices in place to protect the Dallas office building from bomb-laden vehicles were not in use: a gate was unlocked and security bollards were retracted. GSA contract guards did not ensure the gate was locked and the bollards raised after the routine removal of a trash dumpster.
- Bollards were not in place where needed at the Phoenix office building with large ground floor windows and a wide sidewalk. The sidewalk could have been used to park an explosive-laden truck directly against the building. Management was not aware of this potential hazard.
- A shared driveway at the Phoenix office could have been used for a bomb-laden vehicle to enter and park at an unguarded loading dock without detection. Additional guard service or a security camera at the loading dock would improve security but were not employed due to a lack of funding.
- A large sign announcing Internal Revenue Service (IRS) hiring was posted at an intersection on the perimeter of the TCC. The sign defeated the low profile maintained throughout the rest of the facility and drew unnecessary traffic onto the facility grounds as individuals arrived to inquire about employment. Security

management at the facility was aware of this hazard but had not been able to obtain the cooperation of other functional management in its efforts to remove the sign.

- A building directory at the Phoenix office disclosed the location of the computer rooms. Security management was not aware of this hazard but promptly removed the signage.

Perimeter doors were not adequately secured

- Intruders had easy access into the Midtown Manhattan office through fire exit doors and freight elevator doors that were unlocked, propped open, did not properly close, and were either not alarmed or had an alarm that was not functioning. These doors could also serve as exits for an intruder, visitor, or employee to remove computer resources without detection. These conditions occurred because employees were not alert to security vulnerabilities, and Agency-Wide Shared Services (AWSS) staff did not adequately review security controls to ensure that locks and alarms were functioning properly. Also, the AWSS staff did not coordinate with the GSA to have an alarm installed on a fire exit door shared by all building tenants.
- An intruder could have surreptitiously entered and exited the TCC through an unguarded door leading to and from an adjacent child care center. This door was controlled by key card access only. Identification was not checked, bags were not screened, and there was no control in place to prevent an intruder from piggybacking behind an employee to enter the computing center. The lack of a guard at this door could have also allowed an employee or intruder to remove data or computer resources without detection. Management cited a lack of funding to provide full-time guard service at this door.
- The lobby at the Phoenix office was left unguarded at times, and visitors and their bags were not screened through a magnetometer or X-ray machine. A vulnerability assessment conducted at this site concluded that three guards were necessary to adequately secure the lobby. Management cited a lack of funding to hire additional guards as the cause of this on-going vulnerability.

Identification badges and keys were not adequately controlled

- At the Midtown and Downtown Manhattan offices, many employees did not wear identification (ID) badges. This security weakness was caused by a lack of attention to existing security procedures.
- Insufficient controls over electronic key cards, and ID media at the TCC and the Manhattan offices could have allowed an intruder to use these items to gain unauthorized access to facilities and resources. Due to a lack of emphasis on controlling ID badges, the computing center had no inventory listing of presently

assigned keycards, keycards on hand, or keycards destroyed or scheduled for destruction. ID badges were not always returned when employees of the Manhattan offices separated from the IRS. The Security office had discontinued a previous practice of periodically obtaining notification of separated employees from the Personnel function.

- The Grand Master key for the Midtown Manhattan office was cut from a key form that could have been duplicated. A copy of this key, which opens all doors in the building, including the telecommunications equipment rooms, as well as two proximity cards that allow access into the building, were not properly safeguarded while in the possession of the building manager. Security personnel were not aware of the need to use a key form that could not be duplicated and had not periodically inspected the sealed envelope containing the master key and access cards in the building manager's possession to ensure that these items were properly secured.

Computer facilities and data were not adequately secured

- At the Downtown Manhattan office, access to the telecommunications equipment rooms was not sufficiently limited or monitored. Building contractor employees had unescorted and unrestricted access to the telecommunications equipment rooms making the equipment and data vulnerable to damage or theft. Two application servers in this room were left logged on by a system administrator, one of these for 4 days, providing an opportunity for any intruder to cause damage or obtain unauthorized access to systems and sensitive taxpayer data.
- A lack of emphasis on security of magnetic media storage resulted in vulnerabilities at four offices reviewed. There was no inventory of stored magnetic media and no sign-out log for the tape library at the Dallas office. At the Phoenix office, the inventory was inaccurate making it difficult to account for the media. Off-site facilities were not used to store backup tapes for the Midtown and Downtown Manhattan offices to protect the tapes in the event they were needed to restore data.

Appendix V

Management's Response to the Draft Report

TD P 15-71

EPUTY COMMISSIONER

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

RECEIVED
JUL 0 6 2001

July 2, 2001

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: for John C. Reece
Deputy Commissioner of Modernization &
Chief Information Officer

SUBJECT: Response to Draft Report - Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

Thank you for the opportunity to review and comment on your draft report and recommendations concerning our physical security at four IRS facilities. As you know, the IRS has made substantive improvements to the physical security at many of its major facilities, where the IRS has delegation of authority from the General Services Administration to protect persons and property at these locations. In regards to facilities covered by this report, the IRS has a security delegation of authority for the Tennessee Computing Center only. GSA has primary authority and responsibility to protect persons and property at the other four facilities in this review.

The IRS' primary physical security authority and responsibility at these four facilities starts at the perimeter to the IRS space. In this regard, some of the report's findings are not within the total control of the IRS. For example, the newspaper receptacles were located outside of a federal office building where IRS can only request that they be moved. In addition, the security gates and retractable bollards mentioned in the report were federal building perimeter security measures, and are not IRS devices, therefore the Service can only request that they be used. Finally, IRS has limited control over shared driveways. In leased facilities, the Service does have direct authority to implement security measures within the boundaries of the space it occupies. The IRS can only suggest improvements with regards to the building perimeter or common areas within the facility.

TD P 15-71

The IRS, as tenants in GSA-leased facilities, participates as a member of the Building Security Committee. In this forum, the IRS presents instances where improvements in building security are warranted. However, this Committee is run by the concurrence of all members for a corrective action to be implemented. In this regard, the IRS will ensure that the report's findings are communicated to GSA and other committee members.

We appreciate your comments that will further assist us in strengthening our security controls. See the attached detailed response to each of your report recommendations. If you have any questions and/or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of IRS-Wide Security at (202) 622-8910.

Attachment

TD P 15-71

Management Response to Draft Audit Report – Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

RECOMMENDATION #1:

We recommend that the Chief, Agency-Wide Shared Services (AWSS) coordinate with functional managers to place additional emphasis on employee awareness of physical security controls such as the importance of wearing ID badges and being alert to open or unlocked doors and gates and other conditions that place the employees and facilities at risk.

ASSESSMENT OF CAUSE:

Perimeter doors at two offices (Midtown and Downtown Manhattan, New York) were unlocked, propped open, did not properly close, were either not alarmed or had an alarm that was not functioning, or were not properly guarded. These conditions occurred because employees were not alert to security vulnerabilities, and the AWSS staff did not adequately review security controls to ensure that locks and alarms were functioning properly. Also, the AWSS staff did not coordinate with GSA to have an alarm installed on a fire exit door shared by all building tenants. At two offices many employees did not wear ID badges.

CORRECTIVE ACTION TO RECOMMENDATION #1:

1. The New York Metro Facilities Management Branch (FMB) Office will coordinate with IRS managers at the Midtown and Downtown Manhattan offices to ensure they understand the IRS security policy pertaining to wearing identification badges in IRS controlled space and their role in enforcing the policy. Also, the New York Metro FMB office will assist managers in fulfilling their obligation through security awareness training.
2. The New York Metro FMB office will coordinate with Federal Protective Service to remedy the vulnerabilities at the Midtown Manhattan office cause by unsecured doors.

IMPLEMENTATION DATE:

August 1, 2001

RESPONSIBLE OFFICIAL:

Director, Security and Safety Branch, Real Estate and Facilities Management, AWSS, A:RE:S

TD P 15-71

RECOMMENDATION #2:

We recommend that the Chief, Agency-Wide Shared Services (AWSS) place alarms on fire exit doors to discourage employees from opening the doors in non-emergencies and leaving them unsecured.

ASSESSMENT OF CAUSE:

Perimeter doors at two offices were either not alarmed or had an alarm that was not functioning, or were not properly guarded. These conditions occurred because employees were not alert to security vulnerabilities, and the AWSS staff did not adequately review security controls to ensure that locks and alarms were functioning properly. Also, the AWSS staff did not coordinate with GSA to have an alarm installed on a fire exit door shared by all building tenants.

CORRECTIVE ACTION TO RECOMMENDATION #2:
The building where the vulnerabilities were identified is a General Services Administration (GSA) leased facility. Responsibility for building exterior and common area security is jointly shared by GSA, GSA's security arm - the Federal Protective Service (FPS) - and the lessor. GSA administers perimeter and common area security measures, e.g., security of fire exit, through the lease. Federal tenant agencies raise common security concerns to GSA through the facility's Building Security Committee (BSC).

The appropriate entity for correcting this vulnerability is the Federal Protective Service (FPS) via the Building Security Committee (BSC).

IRS' New York Facilities Management Branch Office will notify the Building's Designated Official, FPS and the lessor through the Building Security Committee of the vulnerability.

IMPLEMENTATION DATE:

August 1, 2001

RESPONSIBLE OFFICIAL:

Director, Security and Safety Branch, Real Estate and Facilities Management, AWSS, A:RE:S

TD P 15-71

RECOMMENDATION #3:

We recommend that the Chief, Agency-Wide Shared Services (AWSS) ensure that local AWSS staff regularly evaluate and maintain security controls to ensure they are in place and functioning properly.

ASSESSMENT OF CAUSE:

The weaknesses identified at all sites were attributed to insufficient security reviews by on-site physical security personnel, a lack of funding allocated for security improvements, and the need for improved coordination with the General Services Administration (GSA) at multi-tenant locations. Many of the conditions TIGTA noted had been identified in prior reviews but had not been corrected.

CORRECTIVE ACTION TO RECOMMENDATION #3:

During May 2001, the Security and Safety Branch, Real Estate and Facilities Management, AWSS implemented an improved Security Survey and Risk Assessment Program for IRS facilities. This improved program uses a uniform risk assessment methodology to identify facility threats and weaknesses and to identify appropriate measures to counter those threats and weaknesses. The IRS risk assessment process is recurring on a three-year cycle. AWSS plans to complete the first evolution of assessment by the end of CY 2002. Our Facility Management Branch offices execute the program, which will improve their oversight of security for IRS space at GSA owned or leased facilities.

IMPLEMENTATION DATE:

December 31, 2002

RESPONSIBLE OFFICIAL:

Director, Security and Safety Branch, Real Estate and Facilities Management, AWSS, A:RE:S, for coordination of IRS Risk Assessment program.

TD P 15-71

RECOMMENDATION #4:

We recommend that the Chief, Agency-Wide Shared Services (AWSS) allocate funding to increase guard service, and to implement security controls such as magnetometer and X-ray machines where needed.

ASSESSMENT OF CAUSE:

Magnetometers and x-ray machines were not in areas that TIGTA felt they should be.

CORRECTIVE ACTION TO RECOMMENDATION #4:

GSA's Federal Protective Service (FPS) has primary responsibility for mitigating risks of explosive attacks at all GSA owned or leased facilities, where the IRS is a tenant, except at IRS campuses, where the IRS has a security delegation of authority. Mitigating measures, including guard services, are based on a facility's security level (I through IV) and recurring risk assessments for each facility. FPS coordinates mitigating measures with facility tenants, including the IRS, through a Building Security Committee (BSC) or the GSA lessor.

AWSS has primary responsibility for internal physical security of IRS space at GSA owned or leased buildings/facilities and for all physical security at delegated sites. The IRS has also implemented a recurring risk assessment process to specifically address risks and mitigating measures for IRS space and delegated facilities. AWSS coordinates assessment and mitigating measures with FPS and the BSC or the GSA lessor.

IMPLEMENTATION DATE:

December 31, 2002 – IRS will have assessed its need for magnetometer and X-ray machines.

RESPONSIBLE OFFICIAL:

Director, Security and Safety Branch, Real Estate and Facilities Management, AWSS, A:RE:S, for coordination of IRS Risk Assessment program.

TD P 15-71

RECOMMENDATION #5

We recommend that the Chief, Agency-Wide Shared Services (AWSS) ensure that local AWSS management coordinates with General Services Administration where necessary. While GSA is responsible for correcting physical security weaknesses in buildings housing multiple agencies, AWSS should identify weaknesses and follow up with GSA to ensure improvements are made.

ASSESSMENT OF CAUSE:

The AWSS staff did not adequately review security controls and did not coordinate with GSA to have an alarm installed on a fire exit door shared by all building tenants.

CORRECTIVE ACTION TO RECOMMENDATION #5:

The Security and Safety Branch, Real Estate and Facilities Management, AWSS implemented an improved Security Survey and Risk Assessment Program for IRS facilities. This improved program uses a uniform risk assessment methodology to identify facility threats and weaknesses and to identify appropriate measures to counter those threats and weaknesses. The IRS risk assessment process is recurring on a three-year cycle. AWSS plans to complete the first evolution of assessment by the end of CY 2002. Our Facility Management Branch offices execute the program, which will improve their oversight of security for IRS space at GSA owned or leased facilities.

IMPLEMENTATION DATE:

December 31, 2002 – IRS will have assessed its need for GSA to correct physical security weaknesses in buildings that house multiple agencies.

RESPONSIBLE OFFICIAL:

Director, Security and Safety Branch, Real Estate and Facilities Management, AWSS, A:RE:S, for coordination of IRS Risk Assessment program.

TD P 15-71

RECOMMENDATION #6

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer ensure that local ITS management review access to the telecommunication equipment rooms and ensure access is limited based on need and that visitors sign an access register and are monitored while in the room.

ASSESSMENT OF CAUSE:

The requirements in Internal Revenue Manual 2.1.10.5.5, Telecommunications Systems and Services Security were not being followed.

CORRECTIVE ACTION TO RECOMMENDATION #6:

The Director, Information Systems Field Operations will prepare guidelines to be issued to managers in Information Technology directing them to enforce their security requirements for access to telecommunication equipment rooms.

IMPLEMENTATION DATE:

October 1, 2001

RESPONSIBLE OFFICIAL:

Director, Information Systems Field Operations, M:I:F

TD P 15-71

RECOMMENDATION #7:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer ensure that management at IRS offices remove any signage that draws unnecessary attention to IRS facilities and computer resources.

ASSESSMENT OF CAUSE:

IRS was not in compliance with the Consolidated Physical Security Standards for IRS Facilities (CPSS). The CPSS, which provides a set of minimum physical security standards for IRS facilities, states that receptacles that could conceal explosives should be kept away from the building; passive vehicle barriers, such as security bollards, should be provided at all IRS facilities; and signs indicating the location of sensitive assets should be minimized.

CORRECTIVE ACTION TO RECOMMENDATION #7:

1. Computing Center Directors will remove all signage that draws unnecessary attention to the IRS facility and computer resources.

2. The Office of Security will work with other office heads to ensure unnecessary signage is removed.

IMPLEMENTATION DATE:

September 30, 2001
December 30, 2001

RESPONSIBLE OFFICIAL:

Director, Office of Security Evaluation and Oversight M:S:S

TD P 15-71

RECOMMENDATION #8:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer improve controls to ensure that magnetic media is accounted for and backup tapes are stored off-site.

ASSESSMENT OF CAUSE:

The requirements in Internal Revenue Manual 2.1.10.6.1, Disaster Recovery and Business Resumption Program were not being followed.

CORRECTIVE ACTION TO RECOMMENDATION #8:

The Director, Information Systems Field Operations will issue guidelines to managers in Information Technology directing them to enforce the requirements for proper maintenance of magnetic media inventory and off-site storage of backup tapes.

IMPLEMENTATION DATE:

October 1, 2001

RESPONSIBLE OFFICIAL:

Director, Information Systems Field Operations, M:I:F

TD P 15-71

RECOMMENDATION #9:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer periodically remind employees (for example, through Leave and Earnings Statement flyers) of the proper storing and securing of laptop computers on IRS premises.

ASSESSMENT OF CAUSE:

At one office, 21 laptop computers were not secured during non-duty hours, in violation of IRM requirements for securing portable computers. These conditions occurred because employees did not provide sufficient effort in securing laptop computers.

CORRECTIVE ACTION TO RECOMMENDATION #9:

Action will be taken to ensure that periodic reminders about the proper storage and securing of laptop computers go to employees via communications, including flyers in the Leave and Earnings Statement.

IMPLEMENTATION DATE:

January 1, 2002

RESPONSIBLE OFFICIAL:

Chief, Security Program Office, M:S:C:S

TD P 15-71

RECOMMENDATION #10:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer assign accountability over laptops given to volunteer tax assistors to an IRS employee in each office. Develop procedures to ensure that all laptops issued to volunteer tax assistors are returned to the IRS at the end of the filing season.

ASSESSMENT OF CAUSE:

During the 2001 filing season, more than 5,000 IRS laptop computers were used by volunteers who were, for the most part, not IRS employees. These volunteers prepared and stored approximately 440,000 tax returns on laptop computers. Their portability and value also make laptop computers prime targets for theft. The risk of theft is greater for these computers since the IRS cannot ensure that the laptops are physically secured while in the possession of the volunteers. Three of the offices had poor inventory practices.

CORRECTIVE ACTION TO RECOMMENDATION #10:

Stakeholder Partnership, Education and Communication (SPEC) Territory Managers are assigned the responsibility and accountability over laptops given to volunteer assistors. These managers control their inventory by maintaining inventory certification reports and following procedures as required by Information Technology. SPEC Territory Managers also ensure that taxpayer data is erased from the TaxWise program and any other laptop files at the end of the filing season. The primary methods for accomplishing this are to deinstall the TaxWise program and utilize operating system commands to erase database binary files. SPEC managers will ensure that the VITA site coordinator reinforces the message to protect taxpayer data throughout the filing season and reiterate the need to protect the government owned computer equipment.

SPEC also plans to increase its efforts to ensure that password security features are being used appropriately. We are also exploring the use of automatic file encryption programs for encryption of the hard drives. Action will be taken to also ensure that taxpayer data is erased from the government provided VITA laptops at the end of the filing season. If the equipment is maintained in the field by volunteers, the Territory Managers will be responsible for ensuring that data files are deleted from the computers.

The Director, Stakeholder Partnership, Education and Communication has determined that the recommendation to ensure that all laptops issued to volunteer tax assistors are returned to the IRS at the end of the filing season is not practical and contravenes the congressional mandate to increase the number of e-filed returns to 80% by the year 2007. As more computers are placed in the

TD P 15-71

TD P 15-71

volunteer community to reach the congressional e-file mandate, the space required to store the computers and the number of additional staff years required to set-up, breakdown and transport the computers become prohibitive both in terms of cost and efficiency.

IMPLEMENTATION DATE:

January 1, 2002

RESPONSIBLE OFFICIAL:

Director, Stakeholder Partnership, Education and Communication, W:CAR:SPEC

TD P 15-71

RECOMMENDATION #11:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer establish procedures, in conjunction with the Director, Stakeholder Partnership, Education and Communications, to regularly remove taxpayer data from the hard drives of laptop computers used by volunteer tax assistors, and follow up with the assistors to ensure compliance.

ASSESSMENT OF CAUSE:

The IRS did not require that tax return information stored on the more than 5,000 IRS laptop computers used by volunteers be removed as soon as the electronically filed returns were accepted and the data was no longer needed by the volunteers. Also, a disk wiping utility was not provided to the volunteers to remove taxpayer data before returning the laptops to the IRS at the end of the filing season.

CORRECTIVE ACTION TO RECOMMENDATION #11:

SPEC has determined that the recommendation as it stands is not cost-effective and would severely hamper its ability to attract and retain good volunteers thereby jeopardizing the whole program.

However, to mitigate the risk identified, SPEC is exploring the use of automatic file encryption programs for encryption of all data on the hard drive. SPEC will be working with ITS to see if the packages used by our own Revenue Agents and Officers are compatible with the VITA laptop configurations so that we may take advantage of Service-wide site licenses. We agree that all machines must be cleared of all tax return information at the end of the filing season and we plan to provide further instructions to all Territory Managers requiring removal of the information and destruction of the hard drives on damaged equipment.

IMPLEMENTATION DATE:

July 31, 2002

RESPONSIBLE OFFICIAL:

Director, Stakeholder Partnership, Education and Communication, W:CAR:SPEC