Actions Are Needed to Improve the Effectiveness of the Physical Security Program

March 13, 2008

Reference Number: 2008-20-077

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

March 13, 2008

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Are Needed to Improve the Effectiveness of the Physical Security Program (Audit # 200720030)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has an effective program for managing physical security at its facilities. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of the Information Systems Programs business unit's statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

The IRS has an obligation to protect the Federal Government tax administration system, which includes employees, tax return information, and equipment. Although the IRS has established a means to regularly review physical security controls, management has not ensured that all physical security reviews were completed as required. As a result, potential security risks at various IRS facilities may not be identified and mitigated in a timely manner.

Synopsis

The IRS has developed physical security controls for protecting its employees and taxpayer information. These controls are effective for identifying risks, assessing compliance with controls, correcting weaknesses when identified, and reporting incidents.

Risk assessments and compliance reviews are the primary tools used by the IRS to evaluate the adequacy of physical security controls. However, some risk assessments and compliance reviews have not been completed as required. As of October 25, 2007, IRS employees in the Physical Security and Emergency Preparedness office within the Agency-Wide Shared Services

organization still needed to complete 328 (65 percent) of the 508 required risk assessments and 293 (68 percent) of the 432 required compliance reviews.

In addition, the Physical Security and Emergency Preparedness office had not maintained sufficient information to evaluate the overall IRS physical security program. Records of physical security reviews were not properly maintained and, in some instances, records of these reviews were either lost or misplaced. Also, reports used to monitor completion of the reviews were incomplete, and annual summary reports did not contain cumulative results or statistics to measure accomplishment. Due to these program weaknesses, the IRS cannot provide adequate assurance that the necessary controls are in place to protect employees, facilities, and sensitive taxpayer information. During this review, the Physical Security and Emergency Preparedness office made progress in developing controls to better monitor the IRS physical security program.

Overall, the Physical Security and Emergency Preparedness office has been effective at correcting physical security vulnerabilities identified during the risk assessment process. However, due to limited funding, not all vulnerabilities identified could be corrected. Management has taken appropriate steps to prioritize the necessary corrective actions and fund them as the budget allows. Management has also taken sufficient corrective actions on individual physical security incidents reported to the IRS Computer Security Incident Response Center through the Situation Awareness and Management Center.

Recommendations

To meet the requirements for conducting risk assessments and compliance reviews, we recommended that the Chief, Agency-Wide Shared Services, continue to increase monitoring of physical security activities and analyze current processes and work products. This analysis should focus on identifying methods for completing risk assessments and compliance reviews more efficiently. To better evaluate the IRS physical security program, we recommended that the Chief, Agency-Wide Shared Services, require the Physical Security and Emergency Preparedness office to maintain all required records of physical security reviews and to develop accurate, up-to-date management information with which to better evaluate the IRS physical security program.

Response

Management agreed with our recommendations. The Director, Physical Security and Emergency Preparedness, will increase monthly monitoring and analysis of physical security activities, pursue methods to streamline the risk assessment and compliance review process, and issue guidance requiring employees to forward completed and approved physical security review reports to the Physical Security and Emergency Preparedness Program Office within 30 days of management approval. The Director will elevate to management a list of overdue risk

assessments and compliance reviews. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Abbreviations

IRS	Internal Revenue Service
PSEP	Physical Security and Emergency Preparedness

Background

The Internal Revenue Service (IRS) has an obligation to protect the Federal Government tax administration system, which includes employees, tax return information, and equipment. To meet this obligation, it has developed and documented physical security controls for protecting over 680 IRS facilities. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locked entryways.

The terrorist attacks of September 11, 2001, increased security awareness and brought a shift in the assessment of risks and vulnerabilities. The Treasury Inspector General for Tax Administration has performed two physical security reviews since September 11, 2001.[1] Both reviews outlined a number of security weaknesses and concerns. Recently, the Government Accountability Office recommended additional testing and monitoring of security alarms to increase the functionality of the systems.[2]

An organization as large as the IRS must have an effective physical security program that vigorously assesses risk, monitors compliance with controls, corrects weaknesses when they are identified, and reports and investigates incidents promptly. Physical security program responsibilities within the IRS were historically part of the Real Estate and Facilities Management Office in the Agency-Wide Shared Services organization. In Fiscal Year 2004, responsibility for physical security was moved to the Emergency Management and Physical Security Division in the Mission Assurance and Security Services organization. This effort was to bring together previously separate security functions and enable a consistent, unified approach to physical and information security. On July 8, 2007, the IRS dissolved the Mission Assurance and Security Services organization and transferred responsibility for managing physical security to the Physical Security and Emergency Preparedness (PSEP) office in the Agency-Wide Shared Services organization.

This review focused on management of the IRS' physical security program. We performed the review at the offices of the Chief, Agency-Wide Shared Services, and Chief, Cybersecurity, in Washington, D.C., during the period April through October 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We

[1] *Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail* (Reference Number 2003-20-004, dated October 2002) and *Taxpayer Remittances Were Generally Safeguarded Within the Cincinnati Submission Processing Site; However, Perimeter Security Needs Improvement* (Reference Number 2004-30-183, dated September 2004).
[2] *GAO Management Report: Improvements Needed in IRS's Internal Controls* (GAO-06-543R, dated May 2006).

believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The process used by the PSEP office is generally effective for identifying risks, assessing compliance with controls, correcting weaknesses when identified, and reporting incidents. However, we did identify issues that need to be addressed to enable the IRS to provide more assurance that employees and sensitive taxpayer data are properly protected.

Management Has Developed a Process for Evaluating Physical Security

An effective physical security program requires that security controls be monitored regularly. The PSEP office should consistently ensure that the controls in place comply with existing guidance, align with evolving technologies, support the agency's mission, and accomplish their intended purpose. Risk assessments and compliance reviews are the primary tools used by the PSEP office to evaluate the adequacy of physical security controls in the IRS.

Risk assessments identify internal and external threats. They follow a quantitative process to determine which risks are acceptable or unacceptable. Compliance reviews assess the implementation of security program standards and requirements. The PSEP office should recommend the appropriate controls to reduce risk to an acceptable level.

We selected a judgmental sample of 50 IRS facilities to evaluate the adequacy of physical security reviews conducted for these facilities. At the time of our review, risk assessments were available for 47 of the 50 facilities and compliance reviews were available for 33 of the 50 facilities. Because the remaining 3 risk assessments and 17 compliance reviews could not be located, we assumed they had not been conducted.

Generally, the 80 physical security reviews we analyzed were complete and conformed to IRS policies and procedures. The risk assessments and compliance reviews were conducted using a standardized form to assist the reviewers in covering all security aspects required in a facility's evaluation.

More management involvement is needed to enhance the review process

While the risk assessments and compliance reviews we evaluated were complete, the reviews were not being completed in a timely manner, and sufficient information was not being maintained by management to assess the process.

In October 2006, the Department of the Treasury increased the requirements for conducting risk assessments for certain large facilities from every 3 years or 4 years to every 2 years.[3] Figure 1 depicts the required frequency of both risk assessments and compliance reviews.

Figure 1: Frequency of Required Physical Security Reviews

Building Security Level	Number of Employees or Criticality	Frequency of Risk Assessments	Frequency of Compliance Reviews
Level I	10 or Fewer Employees	Every 4 Years	Every 3 Years
Level II	11 - 150 Employees	Every 4 Years	Every 3 Years
Level III	151 - 450 Employees	Every 3 Years	Every 3 Years
Level IV	451 or More Employees	Every 2 Years	Every 2 or 3 Years[4]
Level V	National Security Critical Infrastructure Assets	Every 2 Years	Every 2 Years

Source: Department of the Treasury and IRS security requirements.

The PSEP office is experiencing delays in conducting required physical security reviews at IRS facilities. To meet the new requirements, the PSEP office needed to complete 508 risk assessments and 432 compliance reviews during the period January 1 through December 31, 2007. As of October 25, 2007, the PSEP office still needed to complete 328 (65 percent) of the 508 risk assessments and 293 (68 percent) of the 432 compliance reviews. It is unlikely that all necessary security reviews will be completed according to the required schedule.

To address the backlog in conducting security reviews and determine the amount of time staff expended on physical security activities, the PSEP office requested that a workload analysis be performed. The analysis, conducted in March 2007, was based on the average physical security workload for 1 year. It provided useful information by identifying the time required to conduct a risk assessment and a compliance review and the number of employees needed to carry out the responsibilities of the program, considering the change in requirements. Management also requested that all PSEP office employees start tracking their time for various tasks beginning in Fiscal Year 2008.

These are positive steps that may help management determine the proper staffing level for the PSEP office. However, before the PSEP office requests more staff, we believe actions should be taken to evaluate the efficiency of the security review process. For example, risk assessments

[3] Department of the Treasury Security Manual, TDP 15-71, dated October 10, 2006.
[4] Compliance reviews should be conducted at least every 3 years for all Level IV IRS facilities. Compliance reviews for Level IV Processing Centers should be conducted every 2 years.

and compliance reviews are currently conducted separately for the same facility. However, it may be more efficient to do them concurrently. Reviewers are also assigned clerical duties such as distributing badges. It may be more efficient to assign those responsibilities to lower grade employees so the reviewers can spend their time conducting risk assessments and compliance reviews.

In addition, the Program Planning and Policy Office in the PSEP office had not maintained the records required to keep track of the reviews that were and were not completed. The three Area Offices[5] in the PSEP office are required to provide annual summaries to present an overview of accomplishments, problem areas, planned program direction, and security initiatives. However, the summary information was generally presented in narrative form, with no cumulative results or statistics to measure accomplishment of planned risk assessments and compliance reviews. The annual summaries showed only the physical security reviews that had been done and did not address any that had not been done.

In April 2007, the PSEP office created a spreadsheet as a control for monitoring the status of risk assessments and compliance reviews. The spreadsheet contained fields to record the date of the most recent review, the date on which the next review was due, and the date on which the next review was scheduled for each of the security reviews. However, as of May 2007, we had identified that 40 percent of the records were blank.

Also, the records of physical security reviews were not properly maintained, and some records of reviews were lost or misplaced. As risk assessments and compliance reviews are performed at IRS offices, copies of these reviews should be forwarded through channels to staff located in the PSEP office at the IRS Headquarters. In October 2006, the PSEP office delegated the custodial duties of collecting and maintaining these records to an employee in [redacted]. This employee is responsible for collecting all physical security review records and maintaining the control spreadsheet. 3(d)

3(d) When obtaining our sample of physical security reviews, we found that, contrary to the process developed by the PSEP office for maintaining security reviews, the records of the reviews were not maintained in [redacted] but rather at multiple offices. As a result, it took the employee in 3(d) [redacted] approximately 4 weeks to gather the security review records from the various IRS offices.

Due to these program weaknesses, the IRS is not adequately assured of having the necessary controls in place to protect employees, facilities, and sensitive taxpayer information. We attribute these weaknesses to a lack of attention by PSEP office management.

During this review, the PSEP office made progress in developing controls to better monitor the physical security program. In September 2007, management provided additional documents

[5] A geographic organizational level used by IRS business units and offices to help their specific types of taxpayers understand and comply with tax laws and issues.

outlining program improvements recently implemented. The PSEP office is now preparing monthly status reports showing the percentages of required security reviews that have been completed. In addition, it now provides quarterly statistics for Business Performance Reviews to the Deputy Commissioner for Operations Support.

The PSEP office is also working to develop a comprehensive performance metrics database to be deployed in Fiscal Year 2008. This database will allow employees to directly load progress data about the completion of risk assessments and compliance reviews for monthly rollup reporting.

Recommendations

The Chief, Agency-Wide Shared Services, should:

Recommendation 1: Continue to increase monitoring of physical security activities, specifically the time expended on compliance reviews and risk assessments, and analyze the current processes and work products. This analysis should focus on identifying methods for completing risk assessments and compliance reviews more efficiently.

> ***Management's Response:*** IRS management agreed with this recommendation. The Director, PSEP, will increase monthly monitoring and analysis to ensure elevation to management of each risk assessment and compliance review that is scheduled and has not been performed. Software will be upgraded to assist security analysts with performing both reviews and ensure that all report requirements are current.

Recommendation 2: Require the PSEP office to maintain all required records of physical security reviews and to develop accurate, up-to-date management information with which to better evaluate the IRS physical security program.

> ***Management's Response:*** IRS management agreed with this recommendation. The Director, PSEP, will issue guidance to all PSEP office employees directing them to forward all completed and approved risk assessment and compliance review reports to the PSEP Program Office within 30 days of management approval. The Director will increase monitoring to ensure that monthly reporting of overdue and currently scheduled reviews is site specific.

Vulnerabilities Identified During Physical Security Reviews Are Properly Prioritized

Although the PSEP office has identified corrective actions to address all physical security vulnerabilities identified during risk assessments, it has not implemented many because of limited funding. The PSEP office has taken appropriate steps to prioritize the necessary corrective actions and fund them as the budget allows.

The PSEP office prepared a Master Fiscal Year 2007 Prioritized Proposed Security Project Listing showing all corrective actions and projected costs. According to the Master Listing, the projected costs of the 119 vulnerabilities that need funding totaled $3,750,000. The PSEP office reported that it is unable to fund corrective actions totaling more than $1,000,000 for 31 (26 percent) of the 119 security vulnerabilities.

However, several of the unfunded items are upgrades of existing equipment, such as access card readers that are scheduled to be replaced in the near future as a result of Homeland Security Policy Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. This Directive requires implementation of a new standardized process for issuing identification badges that is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued Federal Government identification badges. Management made the decision to withhold funding for these actions because a coordinated approach is needed to ensure that the Directive is implemented consistently throughout the IRS.

Reported Security Incidents Have Been Sufficiently Addressed

IRS employees and managers are responsible for reporting individual physical security incidents to the IRS Computer Security Incident Response Center through the Situation Awareness and Management Center, which serves as the IRS' central communications and monitoring facility and is available 24 hours a day, 7 days a week. The incidents are reviewed by PSEP office managers, who should take necessary followup actions on each incident reported. The types of incidents that must be reported include:

- Bomb threats
- Explosions
- Demonstrations
- Civil disturbances
- Fire
- Utility disruption or failure
- Sabotage
- Natural disasters
- Unusual weather conditions
- Terrorist/enemy attacks
- Hazardous materials
- Burglaries
- Robberies
- Thefts
- Destruction or loss of significant documents
- Receipt of information of terrorist activities
- Threats against or assaults upon IRS employees

Our analysis of the incident reports for the period April 1, 2006, through March 31, 2007, identified 1,136 incidents reported to the Computer Security Incident Response Center. Of these, 879 (77 percent) were due to an act of nature or facility/equipment. Only 257 (23 percent) of the incidents reported would possibly require followup action and analysis by the PSEP office. Figure 2 presents an analysis of the types of incidents reported.

Figure 2: Types of Incidents Reported to the Computer Security Incident Response Center

Type of Incident Reported	Number	Percentage
Act of nature	514	45%
Facility/equipment	365	32%
Suspicious package	84	7%
Personnel/taxpayer	61	5%
Hazardous material	23	2%
Bomb threat	19	2%
Loss or theft of non-Information Technology property	19	2%
Suspicious activity	18	2%
Threats (personnel)	18	2%
Other	9	1%
Threats against facilities	5	Less than 1%
Tax data/tax processing equipment	1	Less than 1%
Total	**1,136**	

Source: Situation Awareness and Management Center report "Physical Incidents by Type and Location," dated March 31, 2007.

We reviewed each of the 257 incidents that might require corrective actions to physical security, such as lost badges, missing or damaged equipment, or broken windows and doors. From these, we sampled 27 of the incidents and contacted the respective managers. We confirmed that sufficient corrective actions had been taken in each case.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has an effective program for managing physical security at its facilities. To accomplish our objective, we:

I. Determined whether required physical security reviews were completed at IRS facilities in accordance with Federal Government standards and IRS guidance.

- A. Identified and reviewed updated policies on physical security and data protection requirements and standards.
- B. Interviewed the Program Director in the PSEP office within the Agency-Wide Shared Services organization to determine the processes and standard operating procedures used for managing the IRS' physical security program.
- C. Reviewed IRS physical security Area Office[1] records for Areas 1 and 2.
- D. Selected a judgmental sample of 50 IRS facilities in Areas 1 and 2 from a population of 680 offices, reviewed documentation of risk assessments and compliance reviews conducted for the 50 facilities, and determined whether the assessments and reviews were completed as required. We used a judgmental sample because we were not going to project the results to the population.

II. Determined whether physical security incidents identified at IRS facilities had been sufficiently addressed.

- A. Identified and evaluated the efforts taken to address employee safety and physical security.
- B. Determined whether the PSEP office was effectively monitoring the IRS physical security program at the national level.
- C. Identified all physical security and employee incidents reported to the Computer Security Incident Response Center by type and location for the period April 1, 2006, through March 31, 2007. We identified 257 incidents that indicated corrective actions were required to improve physical security and selected a judgmental sample of 27 to confirm implementation of corrective actions. We used a judgmental sample because we were not going to project the results to the population.

[1] A geographic organizational level used by IRS business units and offices to help their specific types of taxpayers understand and comply with tax laws and issues.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Michelle Griffin, Audit Manager
David Brown, Lead Auditor
Cari Fogle, Senior Auditor
George Franklin, 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 Information Officer OS:CIO
Director, Program Oversight OS:CIO:SM:PO
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 Controls OS:CFO:CPIC:IC
Audit Liaisons:
- Chief, Agency-Wide Shared Services OS:A
- Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report

AGENCY-WIDE SHARED SERVICES

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

RECEIVED
FEB 20 2008

FEB 20 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Norris L. Walker
Director, Physical Security and Emergency Preparedness

SUBJECT: Draft Audit Report – Actions Are Needed to Improve the Effectiveness of the Physical Security Program (Audit #200720030) (i-trak #20008-32811)

Thank you for the opportunity to comment on the subject report. We agree with your recommendations and our corrective actions are attached. We recognize that there are always new approaches we can take to improve our program.

We are pleased with your recognition of our prioritization and use of security funds so we may achieve a consistent, coordinated Servicewide implementation of HSPD-12, and of your acknowledgement that follow-up corrective actions for physical security incidents were taken as appropriate. We attribute these positive results to the many efforts we continue to take to standardize and enforce procedures to improve the IRS Physical Security Program.

We will assess and pursue methods to improve the current risk assessment and compliance review processes to determine if they may be streamlined. We will also continue to improve upon the oversight and maintenance of physical security review documentation and continue to improve upon recently developed management reports to enable us to more effectively evaluate our program.

If you have any questions, please contact me at (202) 622-4025, or you may contact Dennis Ouellette, of my staff, at (202) 622-6035. For matters concerning audit follow-up, please contact Greg Rehak, Agency-Wide Shared Services Office of Finance and Strategy, at (202) 622-3702.

Attachment

Attachment
Draft Report – Actions are Needed to Improve the Effectiveness of the Physical Security Program (Audit 200720030) (i-trak #20008-32811)

RECOMMENDATION #1:
Continue to increase the monitoring of physical security activities, specifically the time expended on compliance reviews and risk assessments, and analyze the current processes and work products. This analysis should focus on identifying methods for completing risk assessments and compliance reviews more efficiently.

CORRECTIVE ACTION:
We agree with the recommendation. We will increase monthly monitoring and analysis to ensure elevation to management of each Risk Assessment and Compliance Review that is scheduled and has not been performed. PSEP will also continue to work with MITS to maintain IT security compliance within the Risk Assessment software upgrade and secure web-site development that is being developed. The current software upgrade is also being designed so that data input into a Risk Assessment that is the same as data in a Compliance Review can be populated into a Compliance Review template, thereby allowing for a more efficient, streamlined process. This will assist security analysts with performing both reviews and ensure that all report requirements are current.

IMPLEMENTATION DATE: December 30, 2008

RESPONSIBLE OFFICIAL:
Director, Physical Security and Emergency Preparedness, AWSS

CORRECTIVE ACTION MONITORING PLAN:
Detailed monthly management reports will be provided to the Director, Physical Security and Emergency Preparedness to assess compliance with TIGTA's recommendation.

Attachment
Draft Report – Actions are Needed to Improve the Effectiveness of the Physical Security Program (Audit 200720030) (i-trak #20008-32811)

RECOMMENDATION #2:
Require the PSEP Office to maintain all required records of physical security reviews and to develop accurate, up-to-date management information with which to better evaluate the IRS physical security program.

CORRECTIVE ACTION:
We agree with the recommendation. We will increase monitoring to ensure that monthly reporting is site specific for all overdue and currently scheduled reviews. Guidance will be issued from the PSEP Director to all PSEP employees directing the requirement to forward all completed and approved Risk Assessment and Compliance Review reports to the PSEP Program Office within 30 days of management approval. Status and Area statistics will continue to be submitted to management.

IMPLEMENTATION DATE: June 1, 2008

RESPONSIBLE OFFICIAL:
Director, Physical Security and Emergency Preparedness, AWSS

CORRECTIVE ACTION MONITORING PLAN:
Detailed monthly management reports will be provided to the Director, Physical Security and Emergency Preparedness to assess compliance with the requirement to submit completed and approved reports to the PSEP Program Office with 30 days of management approval.