Treasury Inspector General for Tax Administration

ACTIONS ARE NEEDED TO IMPROVE THE EFFECTIVENESS OF THE PHYSICAL SECURITY PROGRAM

Issued on March 13, 2008

Highlights

Highlights of Report Number: 2008-20-077 to the Internal Revenue Service Chief, Agency-Wide Shared Services.

IMPACT ON TAXPAYERS

The Internal Revenue Service (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.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS has an effective program for managing physical security at its facilities. This review was included in the TIGTA 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.

WHAT TIGTA FOUND

The IRS has developed effective physical security controls for identifying risks, assessing compliance with controls, correcting weaknesses when identified, and reporting incidents. However, several physical security reviews had not been completed as required.

As of October 25, 2007, IRS employees in the Physical Security and Emergency Preparedness (PSEP) office in 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. Also, the PSEP 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 were either lost or misplaced. In addition, management reports used to monitor completion of the reviews were incomplete. Due to these program weaknesses, the IRS cannot provide adequate assurance that the necessary controls are in place to protect employees, facilities, and taxpayer data.

The PSEP office has been effective at prioritizing, funding, and correcting several physical security vulnerabilities identified during risk assessments, as the budget allows. It has taken sufficient corrective actions on physical security incidents reported to the IRS Computer Security Incident Response Center through the Situation Awareness and Management Center.

WHAT TIGTA RECOMMENDED

The Chief, Agency-Wide Shared Services, should 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. The Chief, Agency-Wide Shared Services, should also require the PSEP office to maintain all required records of physical security reviews and develop accurate, up-to-date management information with which to better evaluate the IRS physical security program.

In their response to the report, IRS officials agreed with the recommendations and stated their plan to take appropriate corrective actions. The Director, PSEP, plans to increase monthly monitoring and analysis of physical security activities, pursue methods to streamline the risk assessment and compliance review process, and issue guidance to all PSEP office employees requiring completed risk assessments and compliance review reports to be forwarded to the PSEP Program Office within 30 days of management approval. The Director plans to elevate a list of overdue risk assessments and compliance reviews to management.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

http://www.treas.gov/tigta/auditreports/2008reports/200820077fr.pdf.

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