



Treasury Inspector General for Tax Administration Office of Audit

COMPUTER SYSTEM ACCESS CONTROLS OVER CONTRACTORS NEED TO BE IMPROVED

Issued on July 24, 2009

Highlights

Highlights of Report Number: 2009-20-108 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) uses contractors to perform a variety of information technology functions, such as developing applications for IRS business operations and maintaining computer operations. To perform these functions, contractors are granted access to IRS computer systems. However, some contractors who no longer had a business need to have access had active user accounts on IRS systems. When contractors are allowed to have unnecessary access to computer systems, the IRS is increasing the risks of exposing taxpayer data to unauthorized disclosure and disruption of system operations.

WHY TIGTA DID THE AUDIT

This review was included in the TIGTA Fiscal Year 2008 Annual Audit Plan as part of the statutory requirements to annually review the adequacy and security of IRS information technology.

WHAT TIGTA FOUND

Despite the IRS' policies and procedures and our previous reports of inadequate oversight of contractor access to IRS computer systems, TIGTA identified system access control issues for contractors. From a sample of 7 IRS systems, TIGTA determined that 53 of 376 contractors had active user accounts but did not have a business need for access to that system. These 53 contractors consisted of contractors whose job duties or access privileges had changed and no longer needed system access, contractors who had separated from the contract with the IRS, and contractors who had never logged onto the system or had not logged onto the system within 45 calendar days. TIGTA also identified 15 contractors whose system access was not deleted in a timely manner upon separation from the contract with the IRS. These contractors' accesses were not removed from systems in a timely manner because responsible officials were not following security procedures and

relied on systemic solutions to disable and delete user access to systems based on inactivity.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer 1) provide appropriate communications to all Contracting Officer's Technical Representatives and managers reinforcing the need to ensure that system accesses are revoked when contractors leave the IRS and that separation of duties is followed, 2) enforce current procedures on all systems by configuring systems to automatically disable and/or delete user accounts when they are not accessed for the appropriate number of days, 3) provide appropriate communications to all Contracting Officer's Technical Representatives and managers to remind them that they have the primary responsibility for providing prompt notification to the responsible organization of any contractor status changes, 4) provide appropriate communications to Contracting Officer's Technical Representatives and managers that the Online 5081 system is the primary system used for authorizing and approving requests for any system access and that system access should not be granted until a contractor or employee has successfully completed a background investigation, and 5) improve accountability over employee and manager adherence with security policies and procedures over contractor system access.

In their response to the report, IRS officials agreed with the recommendations. The Modernization and Information Technology Services Cybersecurity organization plans to coordinate with the Agency-Wide Shared Services Contractor Oversight Group to develop and deliver appropriate communications content to Contracting Officer's Technical Representatives and managers to address the report recommendations. Also, the Modernization and Information Technology Services organization plans to enforce system configuration settings to automatically disable contractor's accounts after 45 calendar days of inactivity and ensure that accounts that are inactive for more than 90 days are deleted or securely incapacitated.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2009reports/200920108fr.pdf>

Email Address: inquiries@tigta.treas.gov
Web Site: <http://www.tigta.gov>

Phone Number: 202-622-6500