



Treasury Inspector General for Tax Administration Office of Audit

ADDITIONAL SECURITY CONTROLS ARE NEEDED TO PROTECT THE AUTOMATED COLLECTION SYSTEM

Issued on March 30, 2010

Highlights

Highlights of Report Number: 2010-20-028 to the Internal Revenue Service Chief Technology Officer and the Commissioners for the Small Business/Self-Employed and Wage and Investment Divisions.

IMPACT ON TAXPAYERS

The Automated Collection System (ACS) is a telephone contact system used by Internal Revenue Service (IRS) employees to perform critical IRS processes such as collecting tax revenues and helping taxpayers resolve their tax issues. The IRS needs to implement additional security controls to protect the ACS and sensitive taxpayer data. The lack of complete security controls increases the risks that taxpayer data could be stolen or computer operations could be disrupted.

WHY TIGTA DID THE AUDIT

The ACS plays a vital role in the IRS collection program. In Fiscal Year 2008, the ACS contributed to the collection of \$4.8 billion (17 percent) of the \$27.5 billion collected by the IRS Small Business/Self-Employed and Wage and Investment Divisions. The overall objective of this audit was to determine whether the IRS has implemented access, audit trail, and configuration management controls to secure the ACS.

WHAT TIGTA FOUND

The IRS configured several access controls for the ACS. For example, the IRS configured the ACS to automatically disable or delete user accounts that are inactive and separated key duties among ACS personnel to limit conflicts of interest. In addition, the IRS configured the ACS to automatically lock out users after three unsuccessful logon attempts and implemented a session lockout control on employee workstations to prevent unauthorized users from gaining access to the ACS when the workstations are left unattended.

However, managers were not reviewing their employees' access privileges and did not always timely remove their employees' user account when the employee transferred to another IRS function. In addition, 6 of our sampled 109 employees' system privileges were not restricted to only those privileges needed to perform assigned duties,

Email Address: inquiries@tigta.treas.gov

Web Site: <http://www.tigta.gov>

and managers did not always document their approval of their employees' access privileges.

The IRS is not capturing all of the required auditable events in ACS audit trails. In addition, the IRS had not developed an overall configuration management plan for the ACS; had not documented and maintained a complete, accurate inventory of the ACS hardware, software, and document configuration items; had not properly documented, tested, and authorized changes to ACS software configuration items; and had not timely corrected high- and medium-risk system vulnerabilities.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Technology Officer:

- 1) make the IRS' current efforts to enhance or replace its online user access control system a top priority;
- 2) instruct the Modernization and Information Technology Services organization to create call site procedures to clarify the capabilities of ACS users' profiles;
- 3) set completion dates and prioritize the work needed to complete the high level and ACS configuration management plans;
- 4) appoint an ACS configuration manager to oversee ACS configuration management activities and protect critical ACS documentation by storing the documents in the required electronic document management system;
- 5) identify key software configuration items and maintain the items in a secure system to allow efficient monitoring;
- 6) ensure the IRS' required change management procedures are followed for all changes to the ACS servers; and
- 7) establish criteria and completion dates for addressing vulnerabilities found on servers.

TIGTA also recommended the Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, instruct ACS managers to review their employees' access privileges annually and remove users' accounts from the ACS when the users transfer to non-ACS functions. Lastly, TIGTA recommended the IRS reinstate the ACS Security Maintenance Report that identifies changes to employees' access levels.

In their response to the report, IRS officials agreed with most recommendations and stated it has already revised some procedures. The IRS disagreed with the recommendation to appoint an ACS configuration manager and stated it is currently aligning with configuration management procedures to implement corrective actions. TIGTA continues to believe an ACS configuration manager should be appointed and the weaknesses identified in the report could persist without appointment of this responsible official.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2010reports/201020028fr.pdf>.

Phone Number: 202-622-6500