



Treasury Inspector General for Tax Administration

EFFECTIVENESS OF ACCESS CONTROLS OVER SYSTEM ADMINISTRATOR USER ACCOUNTS CAN BE IMPROVED

Issued on September 19, 2007

Highlights

Highlights of Report Number: 2007-20-161 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

To perform their job responsibilities, system administrators must be given total control over computer systems. Due to the sensitive nature of the administrator position, the Internal Revenue Service (IRS) must have proper controls in place to ensure only appropriate employees have administrator rights and privileges, administrator user accounts are reviewed annually for continued business need, their user accounts are protected with strong passwords, and their actions on computer systems are monitored for questionable activities. However, administrator user accounts were not always authorized and maintained properly, and administrator activities were not consistently reviewed and documented. Weak controls over user accounts could allow unauthorized individuals to gain access to these accounts, which could lead to unauthorized disclosure of taxpayer data and disruptions of service affecting work productivity and revenue collection.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's statutory requirements to annually review the adequacy and security of IRS technology. The overall objective of this review was to determine the effectiveness of access controls over system administrator user accounts on IRS computers.

WHAT TIGTA FOUND

The IRS has over 260 computer system applications to process tax records for 130 million taxpayers and to support and assist its employees in administering the nation's tax system. While the IRS has established appropriate procedures for authorizing and maintaining administrator user accounts as well as procedures to review their user account activities for improprieties, TIGTA identified weaknesses. These weaknesses occurred because managers and system administrators did not adhere to procedures.

Email Address: Bonnie.Heald@tigta.treas.gov

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

First, the IRS is not approving and maintaining proper documentation for establishing administrator user accounts. TIGTA could not find authorization and approval documentation for 31 (5 percent) of 607 user accounts for the 5 applications it reviewed. While 5 percent may seem low, the capabilities of these user accounts magnify the risk because they have unlimited control over computers. Second, the IRS had unnecessary administrator user accounts. Seventy-nine (13 percent) of 607 active user accounts were not needed because the employees no longer had a business need to administer their respective computer systems. Third, weak passwords on user accounts existed on all five applications because systemic password controls did not adhere to required IRS password standards. Finally, system administrator activities were not being monitored for questionable activities for four of the five applications reviewed.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Information Officer ensure managers identify system administrator user accounts on all applications that do not have proper authorization documentation, assess whether the accounts are still needed, and establish appropriate authorization documentation for those accounts; test the automated computer programs (scripts) used to deactivate and/or delete administrator user accounts with periods of inactivity; reinforce the need for managers of system administrators to be cognizant of the applications their employees can access and limit those access rights to only those applications needed to carry out their responsibilities; and ensure the deployment of the host-based intrusion detection software continues to ensure questionable activities from system administrator user accounts on Tier 2 Unix-based servers are captured and reviewed.

In their response to the report, IRS officials agreed with the recommendations. The IRS plans to implement a process to review system administrator user accounts on all systems at least annually to ensure only those system administrator user accounts with a continued business need exist on IRS systems, implement the feature of the operating systems to identify and delete all system administrator user accounts with no activity for 45 days, and send a notice to all managers of system administrators to reinforce the need to be aware of the applications their system administrators can access and to limit those access rights to only those applications needed to carry out their responsibilities. In addition, the IRS plans to deploy Host-based Intrusion Detection Sensor agents on Tier 2 Unix-based servers.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2007reports/200720161fr.pdf>

Phone Number: 202-927-7037