



Treasury Inspector General for Tax Administration Office of Audit

ACCESS CONTROLS FOR THE AUTOMATED INSOLVENCY SYSTEM NEED IMPROVEMENT

Issued on May 16, 2011

Highlights

Highlights of Report Number: 2011-20-046 to the Internal Revenue Service Commissioner for the Small Business/Self-Employed Division and the Chief Technology Officer.

IMPACT ON TAXPAYERS

Bankruptcy petitions filed in Federal courts were up 32 percent in Calendar Year 2009 compared to Calendar Year 2008. The Internal Revenue Service (IRS) receives notification of a bankruptcy case because taxpayers are required to list their creditors and liabilities when filing for bankruptcy protection. The IRS inputs the taxpayers' sensitive information into its Automated Insolvency System (AIS) to track the legal requirements for dealing with the taxpayers and to protect the Government's financial interest. Unauthorized access to the AIS could jeopardize taxpayers' legal rights.

WHY TIGTA DID THE AUDIT

This audit was initiated because the Small Business/Self-Employed Division requested that TIGTA review the access controls for the AIS. The objective of the review was to determine whether the IRS implemented access controls for the AIS to protect taxpayers' personal data and to ensure the Government's interest is protected when taxpayers file for bankruptcy.

WHAT TIGTA FOUND

Although some AIS access controls are in place, such as the automatic lockout control and password complexity settings, other required access controls have not been implemented or are not operating effectively.

TIGTA found many IRS employees have excessive privileges on the AIS. The excessive privileges are due to two primary reasons. First, managers did not ensure duties were adequately segregated among employees to prevent and detect unauthorized activities. The second reason is due to the inadequate role-based access control scheme that was developed for the AIS. The inadequate access control scheme causes managers to inadvertently

grant unneeded, excessive AIS privileges to employees.

TIGTA also found IRS managers and user administrators were not following the requirement to use the Online 5081 system to authorize and revoke access to the AIS. In addition, some significant actions taken on bankruptcy cases are not logged and reported in the AIS Manager Review screen to allow managers to detect errors and inappropriate activities.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, Small Business/Self-Employed Division, 1) identify incompatible duties and implement policies to segregate those duties; 2) issue a memorandum to Insolvency office managers requiring them to adhere to the new policy when assigning duties and approving AIS access rights; 3) define and document user requirements for the AIS based on employee job functions and position descriptions and submit these requirements to the Applications Development office in a formal work request; and 4) issue a memorandum to managers emphasizing the requirement to use the Online 5081 system to authorize, revoke, and review employees' AIS access authorizations.

TIGTA also recommended that the Associate Chief Information Officer, Applications Development, 1) ensure application developers have read-only access to the AIS, 2) develop software to systemically create and assign passwords for new AIS users, and 3) create a role-based access control scheme for the AIS.

The IRS agreed with the recommendations and stated it had already taken two corrective actions. The IRS initiated a work request to develop a self-service password reset and auto generation feature for the AIS. In addition, the User Administrator privilege was removed from the Developer privilege level.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2011reports/201120046fr.pdf>.