



Treasury Inspector General for Tax Administration Office of Audit

ADDITIONAL SECURITY IS NEEDED FOR ACCESS TO THE REGISTERED USER PORTAL

Issued on March 31, 2010

Highlights

Highlights of Report Number: 2010-20-027 to the Internal Revenue Service Chief Technology Officer and Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

The use of the Internet is an integral part of the Internal Revenue Service (IRS) mission to deliver top quality service to all taxpayers. The IRS developed the Registered User Portal (RUP) to provide web access to the IRS' e-Services applications and provide outside tax professionals with the ability to submit and retrieve tax-related information and electronically file (*e-file*) tax returns. Because these external users can access taxpayer data, modify electronic tax returns prior to transmitting them to the IRS, and download taxpayer data to their computers, access controls at the RUP are critical to minimize the risk of unauthorized access to taxpayers' personal tax data.

WHY TIGTA DID THE AUDIT

This audit was initiated because access to the RUP and e-Services applications poses significant risks to the security of taxpayers' personal data. During the IRS' 2008 Filing Season, 58 percent of all tax returns, nearly 90 million of the 155 million tax returns filed, were received electronically.

WHAT TIGTA FOUND

Although some RUP access controls are in place, several other security controls were not implemented. Specifically, suitability checks are not performed on all users who *e-file* tax returns and access taxpayer data. The IRS allows principals and responsible officials at tax preparation firms to delegate their access rights to other individuals. These "delegates" may be members of the firm or persons with whom the firm has a business relationship and do not undergo a suitability check. The IRS also did not follow its procedures for approving *e-file* applicants who failed the criminal background part of their suitability check.

TIGTA found that limitations in the Third Party Data Store, which is used to record and monitor information about individuals who have applied to

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

participate in the *e-file* program, prevent this system from posting the complete results of the systemic tax compliance check that is performed on an applicant's spouse. TIGTA also found that the RUP was not configured to disable and remove users' inactive access accounts in accordance with IRS security policies.

In addition, required password controls were not implemented, a control to permanently lock out users after three unsuccessful logon attempts was not implemented, and the RUP audit logs were not analyzed to detect unauthorized activities.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, 1) require suitability checks on delegated users who *e-file* tax returns or access sensitive e-Services applications; 2) revise the appeal procedures for *e-file* applicants who fail their suitability check to specify that the IRS Criminal Investigation Division's Fraud Detection Center has the final approval authority; 3) disable and delete inactive RUP accounts in accordance with IRS procedures or follow the IRS risk-based decision procedures to obtain the required thorough assessment and approval to not implement these security controls; 4) request the Chief Technology Officer enhance the RUP to require passwords to contain a mix of lower case and upper case letters, set the password length to 12 characters, and prevent the use of Social Security Numbers as usernames; and 5) request the Chief Technology Officer implement a control to allow users to answer a series of challenge questions to unlock their RUP accounts. TIGTA also recommended the Chief Technology Officer 6) enhance the *e-file* application on the Third Party Data Store to post the complete results of the tax compliance check that is performed for an *e-file* applicant's spouse, and 7) develop a process to analyze the activities of RUP users and begin reviewing the audit logs.

In their response to the report, IRS officials agreed with most of the recommendations and stated the RUP audit logs are now being reviewed to detect unauthorized activities. In addition, the IRS plans to establish an Executive Review Board to formally consider deviations from the Criminal Investigation Division's recommendations, and it revised its required minimum password length to eight characters for all systems except the Windows operating system. TIGTA concurs with these corrective actions.

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/201020027fr.pdf>.

Phone Number: 202-622-6500