Treasury Inspector General for Tax Administration
Office of Audit

THE OFFICE OF RESEARCH, ANALYSIS, AND STATISTICS NEEDS TO ADDRESS COMPUTER SECURITY WEAKNESSES

Issued on September 17, 2008

Highlights

Highlights of Report Number: 2008-20-176 to the Internal Revenue Service Director, Office of Research, Analysis, and Statistics

IMPACT ON TAXPAYERS

Information technology personnel in the Internal Revenue Service (IRS) Office of Research, Analysis, and Statistics (RAS organization) manage computer systems that users query to obtain enormous amounts of taxpayer data. However, security weaknesses existed on each of the three computer systems TIGTA reviewed. These weaknesses increase the risks of unauthorized disclosure of taxpayer data and significant disruption to computer operations.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's statutory requirement to annually review the adequacy and security of IRS technology. The overall objective was to determine whether the RAS organization maintained effective security controls over its information systems.

WHAT TIGTA FOUND

TIGTA identified several weaknesses in the management of access to the RAS organization's computer systems. Managers and system administrators had not placed sufficient emphasis on maintaining the security and privacy of the taxpayer data they were charged with protecting. Managers did not carry out their responsibilities to ensure that 1) users were authorized to access the computer systems, 2) access accounts for former employees and current employees who no longer needed access were removed, and 3) system administrators removed or locked unnecessary generic or shared administrator accounts that provide additional opportunities for intruders to gain access to the systems.

In addition, password settings did not conform to IRS information security standards. For example, passwords were not always sufficiently complex, passwords were not set to expire after the required length of time, and new users were not required to change their passwords at initial login.

Unencrypted sensitive data were transferred between computers.

Controls to detect inappropriate security events were not effective. For example, TIGTA found that audit logs were not adequately retained or reviewed. Intrusion detection systems were not installed and virus protection software was not current. In addition, data received from other sources were not scanned with virus protection software before being uploaded to the server.

TIGTA also identified database security vulnerabilities within the systems reviewed. Database patching was not adequate, access permissions were set incorrectly, password settings were incorrect, and the auditing feature was not properly enabled to detect unauthorized activities in the databases. TIGTA also found that system backup files were not stored offsite.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Director, Office of Research, Analysis, and Statistics, 1) designate a security officer to monitor compliance with IRS security requirements and remind managers and employees of their security responsibilities, 2) require system administrators and managers to ensure that all system access controls are followed, and to follow up on identified security weaknesses to ensure that they are corrected in a timely manner, 3) coordinate with the Modernization and Information Technology Services organization to implement secure processes for transferring sensitive data between computers, and ensure that scanning software is used to periodically scan the systems for security weaknesses, 4) implement and monitor a process by which managers validate that system access is limited to only those who have a need, 5) ensure that audit and accountability controls are sufficient by requiring that audit logs are maintained a minimum of 6 years and are reviewed by the security officer, 6) require managers to ensure that offsite storage is used for system and data backup files, and 7) coordinate with the Chief Information Officer to verify that intrusion detection systems are installed to protect all systems and that virus protection software is current.

IRS officials agreed with the findings and recommendations and reported they have already taken many corrective actions to address the recommendations.

READ THE FULL REPORT

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

http://www.treas.gov/tigta/auditreports/2008reports/200820176fr.pdf