



Treasury Inspector General for Tax Administration

STANDARD DATABASE SECURITY CONFIGURATIONS ARE ADEQUATE, ALTHOUGH MUCH WORK IS NEEDED TO ENSURE PROPER IMPLEMENTATION

Issued on August 22, 2007

Highlights

Highlights of Report Number: 2007-20-129 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

Database security controls are an organization's last line of defense in protecting sensitive data. While the Internal Revenue Service's (IRS) standard database security configurations are adequate, they are not effectively implemented on critical databases. Failure to adequately secure these databases places nearly all individual and business taxpayer accounts at risk of unauthorized access, which can lead to identity theft or fraud.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's statutory audit coverage and is included in our Fiscal Year 2007 Annual Audit Plan. IRS databases contain some of the most sensitive information in the Federal Government – taxpayer personal and financial information. While security of any computer system is dependent on the number and strength of the layers of security protecting it, the last and possibly best line of defense in protecting data are database security controls. This review was conducted to determine whether the IRS' standard database security configurations were adequate and effectively implemented.

WHAT TIGTA FOUND

The IRS issued standard security configurations for all IRS databases in March 2006. TIGTA found these configurations to be adequate, since they are aligned with Federal Government guidelines and best practices.

To determine whether the IRS' standard database security configurations were effectively implemented, TIGTA tested basic database security controls on databases from eight tax administration applications. Collectively, these databases failed 30 percent of the tests. Exploitation of the vulnerabilities found could result in unauthorized accesses to taxpayer

information and ultimately result in identity theft or fraud.

The control weaknesses occurred because standard database security configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and tests to detect noncompliance with standard configurations were inadequate.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Information Officer ensure database security control weaknesses identified are corrected and re-publicize standard database security configurations. In addition, the Chief Information Officer should ensure security and administration responsibilities are properly assigned for all IRS databases and investigate alternatives for ensuring employees are aware of their database security responsibilities, with managers holding their employees accountable for meeting those responsibilities. TIGTA also recommended the Chief Information Officer ensure security testing evaluates compliance with standard database security configurations and develop an implementation plan and standard operating procedures for its database compliance assessment tool.

In management's response to the report, the Chief Information Officer agreed with the recommendations. Specific database weaknesses identified in this review will be added to corrective plans of actions and milestones. The IRS' standard database security configurations will also be re-communicated throughout the organization. The Chief Information Officer also plans to assign a project officer and develop a project plan to coordinate activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems, including activities to ensure all IRS databases have individuals assigned to specifically perform security and administration responsibilities. Quarterly reviews will be performed to ensure compliance with IRS policy for these responsibilities, with noncompliance reported to IRS executives for appropriate action. The Chief Information Officer also agreed to include standard database security configurations in the list of controls tested annually. An implementation plan and procedures will also be developed for the IRS' database compliance assessment tool.

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/200720129fr.pdf>.

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

Phone Number: 202-927-7037