



## Treasury Inspector General for Tax Administration Office of Audit

### SECURITY OVER DATABASES COULD BE ENHANCED TO ENSURE TAXPAYER DATA ARE PROTECTED

Issued on May 4, 2011

## Highlights

Highlights of Report Number: 2011-20-044 to the Internal Revenue Service Chief Technology Officer.

### IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) uses more than 2,200 databases to manage and process its taxpayer data. Databases are increasingly being targeted by attackers. When the right degree of security diligence is not applied to databases, disgruntled insiders or malicious outsiders can exploit security weaknesses over databases and may gain unauthorized access to taxpayer data, resulting in identity theft or fraud.

### WHY TIGTA DID THE AUDIT

This review was included in TIGTA's Fiscal Year 2010 Annual Audit Plan and is part of our statutory requirements to annually review the adequacy and security of IRS information technology. This audit also addresses the major management challenge of Security of the IRS. The overall objective of this review was to determine whether the IRS adequately configured databases operating in its non-mainframe production environment to properly secure taxpayer data.

### WHAT TIGTA FOUND

TIGTA found that non-mainframe databases containing taxpayer data were not always configured in a secure manner and that databases were running out-of-date software that no longer received security patches and other vendor support.

In addition, the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise. Also, the IRS purchased a database vulnerability scanning and compliance assessment tool without the completion of adequate product evaluation and testing. As a result, the IRS spent more than \$1.1 million in software licenses and support costs for a tool that was not fully implemented.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure: 1) the security vulnerabilities identified on databases are remediated; 2) explicit management

*Email Address:* [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

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

approvals are included in the database configuration building process; 3) a strategic plan is developed to address outdated database versions; 4) outdated databases are upgraded, planned to be migrated to newer versions, or properly approved to deviate from existing standards; 5) database vulnerability scans are conducted as required by policies; 6) database vulnerability scans test all high- and medium-risk configuration settings; and 7) a thorough technical product evaluation is consistently conducted and documented for the purchase of future software products.

In its response to the report, the IRS agreed with TIGTA's recommendations. The IRS plans to:

- 1) develop a strategy to ensure vulnerabilities are documented;
- 2) identify appropriate organizations to develop a management approval process to be used in the database build and configuration change processes;
- 3) develop a strategic plan for obsolescence of technology, including database version control;
- 4) develop a migration plan to upgrade database software to supported versions;
- 5) establish a process for conducting monthly scans of databases;
- 6) establish a Memorandum of Understanding to ensure database vulnerability scans are conducted with the privileges necessary to test all high- and medium-risk database configuration settings; and
- 7) create/designate a location to ensure all Product Evaluation and Selection and testing documentation is accessible from a centralized location.

The IRS disagreed with TIGTA's \$1.1 million outcome measure related to the licensing of the IRS vulnerability scanning tool. TIGTA maintains the appropriateness of the measure.

### 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/201120044fr.pdf>.

*Phone Number:* 202-622-6500