



## Treasury Inspector General for Tax Administration Office of Audit

### THE MAINFRAME DATABASES REVIEWED MET SECURITY REQUIREMENTS; HOWEVER, AUTOMATED SECURITY SCANS WERE NOT PERFORMED

Issued on September 30, 2011

## Highlights

Highlights of Report Number: 2011-20-099 to the Internal Revenue Service Chief Technology Officer.

### IMPACT ON TAXPAYERS

Internal Revenue Service (IRS) mainframe computers support applications associated with processing, tracking, and storing tax return information. Two manufacturers of mainframe computers, International Business Machines Corporation (IBM) and Unisys Corporation, provide the foundation for the IRS computer systems. TIGTA tested the security configurations of two applications processed with DB2 databases residing on IBM mainframes and found them to be effective; however, automated security scans of the 32 IBM DB2 database applications were not performed. By not performing monthly automated database scans, sensitive information may not be secure.

### WHY TIGTA DID THE AUDIT

In Fiscal Year 2009, the IRS processed about 144 million individual income tax returns and about 2.5 million corporate income tax returns. This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Modernization. Our overall objective was to determine whether adequate security controls were established for the IBM DB2 databases running on the IBM z/OS operating system.

### WHAT TIGTA FOUND

Security policies and configuration settings for the two IBM DB2 databases reviewed were in compliance with Government and industry standards and were effectively implemented. However, required automated security configuration scans of mainframe databases were not conducted. The audit also identified that the IBM Guardium software application purchased in July 2010 for vulnerability scans on databases had not been fully implemented. In June 2011, the IRS received an invoice for approximately \$700,000 to renew the annual software application license. This invoice was paid in order to continue deployment and avoid penalties for a lapse in

maintenance; however, the application had not been fully implemented, resulting in an inefficient use of resources.

### WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer implement automated security configuration scanning on mainframe databases, ensure the IBM Guardium software application is fully implemented, and ensure system requirements are identified and agreed upon by all affected Modernization and Information Technology Services organizations prior to purchasing an enterprise-wide software application.

In their response to the report, IRS officials agreed with all of our recommendations. The IRS plans to implement automated security configuration scanning on mainframe databases and coordinate with stakeholders to fully implement the IBM Guardium software application. Vendor Contract Management plans to ensure that all appropriate information technology stakeholders involved in the acquisition of enterprise software applications have been effectively engaged in the articulation of requirements for new enterprise-wide software applications.

The IRS stated that they did not concur with the outcome measure of \$700,000, as the invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance. However, TIGTA maintains that the inefficient use of resources is due to the delayed deployment that resulted from the lack of proper planning and coordination between the Modernization and Information Technology Services business units prior to the purchase of the application.

### 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/201120099fr.pdf>