



Treasury Inspector General for Tax Administration Office of Audit

INTEGRATED FINANCIAL SYSTEM UPDATES ARE IMPROVING SYSTEM SECURITY, BUT REMAINING WEAKNESSES SHOULD BE ADDRESSED

Issued on March 28, 2013

Highlights

Highlights of Report Number: 2013-20-030 to the Internal Revenue Service Chief Financial Officer and Chief Technology Officer.

IMPACT ON TAXPAYERS

The Integrated Financial System (IFS) is the IRS's core financial system and annually assists the IRS in accounting for approximately \$12 billion in operational funds. The IFS was implemented as a major project under the IRS's Business Systems Modernization Program, but in November 2005 the system was reclassified as Operations and Maintenance funding. For Fiscal Years 2012 and 2013, the IRS requested nearly \$37.5 million to upgrade the IFS. Recently, the IRS initiated approximately \$10.5 million in system updates for the IFS that include: 1) encryption of graphical user interface traffic, 2) update of the platform with functional enhancements, and 3) support of a Department of the Treasury mandate for all Federal agencies. The IRS plans to complete deployment of these system updates in November 2012.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS has adequately planned for the recent updates of the IFS to support long-term goals and to mitigate risks in accordance with the Department of the Treasury, IRS, and other systems development guidelines. TIGTA evaluated key management controls and processes, project funding, and system security risks.

WHAT TIGTA FOUND

In July 2012, the IRS implemented the System Application and Products Secure Network Connection, providing for data encryption and eliminating security weaknesses in the Citrix and IFS Windows 2000 environments. With successful implementation of System Application and Products Enterprise Central Component 6.0, the IRS expects that the IFS will be in compliance with current Federal laws and accounting standards and will address the security weakness related to Oracle database software.

As planned, IFS updates address compliance for specific information technology security controls. However, improvements are needed to better ensure that: 1) remaining IFS security weaknesses are adequately addressed and 2) system requirements testing consistently complies with established IRS guidelines.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer work with the Chief Financial Officer to: 1) apply existing or implement additional access controls to ensure that IFS users are restricted to IRS employee sensitive data on a "need to know" basis; 2) implement control checks to prevent IFS users from accessing unauthorized IRS employee accounts, or prepare a risk-based decision and accept the risk; 3) implement two-factor authentication in a future release and identify a form of multifactor authentication for IFS system administrators; 4) ensure that all applicable system requirements for IFS test cases include expected results; and 5) ensure that all IFS testers obtain and maintain documentation to verify test case results.

In their response to the report, IRS officials agreed with our recommendations. The IRS plans to restrict access to sensitive employee data to only those users with a "need to know" basis; evaluate the identified low risk to determine if a risk-based decision is needed; implement the new version of the Secure Network Connection module once its certification is completed in late 2013; ensure that the IFS is included in the current program-level mitigation strategy to implement two-factor authentication; and link its Rational Quality Manager to its requirements repository so that requirements test management can be properly documented.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2013reports/201320030fr.pdf>.