



Treasury Inspector General for Tax Administration Office of Audit

THE INTERNAL REVENUE SERVICE SHOULD IMPLEMENT AN EFFICIENT INTERNAL INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM THAT MEETS ITS SECURITY NEEDS

Issued on September 17, 2014

Highlights

Highlights of Report Number: 2014-20-083 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The IRS is in the process of implementing an Information Security Continuous Monitoring (ISCM) program. When fully implemented, the program will allow the IRS to continuously monitor security controls of its computer assets in real time, thus improving the effectiveness of the safeguards and countermeasures to protect taxpayer information and information systems.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to assess the current state of Continuous Diagnostics and Mitigation (CDM) program controls in place.

WHAT TIGTA FOUND

Although implementation of the ISCM program has been slow across the Federal Government, the IRS has been in compliance with Department of Homeland Security and Department of the Treasury guidelines.

In addition to the mandatory guidelines imposed by the Office of Management and Budget, Treasury Department officials have also mandated that their bureaus use only the Treasury Department's dashboard that will serve as the official reporting for the ISCM program and use those security tools selected by Treasury Department officials for consistency.

Although the Treasury Department's intentions for consistency and efficiency are workable for most of its offices and bureaus, TIGTA found that, based on the large scale of the IRS's computer environment, a one-size-fits-all approach does not provide the best security for the IRS. TIGTA also identified inefficiencies the IRS will experience if it selects the recommended Treasury Department tool.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS Chief Technology Officer continue to move forward and coordinate, as appropriate, with the Treasury Department to implement a stronger internal ISCM program that allows executives to make the most informed decisions that affect the security of the IRS network. This includes:

- 1) selecting and implementing an internal dashboard,
- 2) taking advantage of the General Services Administration's Blanket Purchase Agreement through the Department of Homeland Security's CDM program to acquire products to ensure that gaps in coverage and tool enhancements of the ISCM program are adequately addressed and best suited for the IRS environment, and
- 3) ensuring that tools selected for use (such as the database scanning tool) are the most effective and make the most efficient use of IRS resources.

IRS officials agreed with our recommendations and plan to continue to coordinate with Treasury to ensure that the IRS selects the most effective and efficient security tools that meet the unique needs of the IRS computing environment. The IRS also plans to take advantage of the General Services Administration's Blanket Purchase Agreement to acquire products to ensure gaps in coverage and tool enhancements are best suited for the IRS environment.

The IRS also plans to establish an enterprise-wide ISCM integrated project team to direct the selection and implementation of an integrated dashboard of the security scanning tools to ensure that stakeholders and decision makers are well-informed to make risk-based decisions and to pursue tool enhancements for current tools and tool selections for gaps to ensure that the most cost-efficient method is used to the extent that funding is available.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2014reports/201420083fr.pdf>.

E-mail Address: TIGTACommunications@tigta.treas.gov

Phone Number: 202-622-6500

Website: <http://www.treasury.gov/tigta>