Treasury Inspector General for Tax Administration
Office of Audit

MEASURABLE AGREEMENTS ON SECURITY CONTROLS ARE NEEDED TO SUPPORT THE ENTERPRISE STORAGE SERVICES SOLUTION

Issued on October 30, 2015

Highlights

Highlights of Report Number: 2016-20-002 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Enterprise Storage Services (ESS) Program is sponsored by the IRS Storage Program Management Office. This office delivers data storage services to Enterprise applications at IRS facilities through deployment of tiered storage, encrypted backup/recovery, and data replication strategies that enable high-performance systems operations, business continuity, and dynamic and secure disaster recovery. The IRS estimates that its new "Storage-As-a-Service" approach will save millions of dollars by providing better utilized resources. The new ESS environment stores IRS data, including taxpayer and other sensitive data.

WHY TIGTA DID THE AUDIT

The overall objective was to assess the efficiency and effectiveness of the IRS's ESS Program by considering progress toward established goals and the risk mitigation approach for the enterprise-wide cloud storage services that support IRS systems and information technology operations.

WHAT TIGTA FOUND

The IRS has reported cost savings with its migration of production data into the ESS storage environment since March 2013.

However, TIGTA found that more detailed contractual agreements are needed to support the ESS Program with data security controls including security monitoring and incident management. Clear agreements between the IRS and the ESS contractor would better ensure adequate preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Also, the Service Level Objectives established under the current contract do not clearly stipulate time frames for the contractor to mitigate losses and resecure the ESS environment should a data breach occur.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS Chief Technology Officer: 1) modify the ESS contract to include measurable Service Level Agreements based on a complete risk assessment and security plan for the ESS Program and 2) address specific risks affecting IRS systems related to ESS security monitoring and incident management.

The IRS disagreed with both recommendations, stating that the ESS provides disk storage as one component of a larger, multilayered infrastructure. Risk and security of all data, including access to the data in addition to IRS incident management and security monitoring, are performed at the General Support System and Application layers using IRS standard practices and processes.

TIGTA believes that risk factors associated with contract responsibilities and ownership of ESS data storage devices should be considered under the ESS Program. IRS policy requires risk management for all infrastructure equipment capable of storing or transmitting data. However, a risk assessment has not been conducted, and the security plan is not complete. Further, the IRS has not provided TIGTA with verification that security controls to address specific ESS risks have been considered at the General Support System and Application layers. The ESS contract does not include or reference a detailed process to guide security monitoring and overall incident management controls.

READ THE FULL REPORT

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

http://www.treas.gov/tigta/auditreports/2016reports/201620002fr.pdf.