



Treasury Inspector General for Tax Administration Office of Audit

BETTER COST-BENEFIT ANALYSIS AND SECURITY MEASURES ARE NEEDED FOR THE BRING YOUR OWN DEVICE PILOT

Issued on September 24, 2013

Highlights

Highlights of Report Number: 2013-20-108 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Bring Your Own Device (BYOD) is a popular trend in mobile computing that allows users to access network resources on their personal mobile devices, such as smartphones. While BYOD has the potential to provide organizations with cost savings, increased productivity, and improved employee satisfaction, mobile devices often need additional protection due to threats of theft and malware exposure. The IRS must ensure that implementing a BYOD program would be cost effective and that any increased risks to the privacy and integrity of taxpayer data can be mitigated.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to evaluate the IRS's costs, administration, and security for its BYOD efforts.

WHAT TIGTA FOUND

The IRS has taken several noteworthy actions to implement its BYOD pilot, including taking a phased approach and considering security. However, although it has spent more than \$900,000 on mobility efforts to date, the IRS has not developed a complete cost-benefit analysis to fully justify the implementation of the BYOD concept within the IRS.

Federal-level guidance states that BYOD should be cost effective and that a cost-benefit analysis is essential. While the IRS did prepare a simple cost analysis that compared the estimated cost of BYOD to the cost of the IRS's existing mobility programs prior to starting the BYOD pilot, it was not updated with complete information on assumptions and costs. BYOD could provide significant benefits; however, these benefits are just conjecture until the IRS conducts a thorough cost-benefit analysis.

Additionally, increased attention is still needed to address security concerns related to the 460 users participating in the BYOD pilot. The IRS allows BYOD devices access to resources on the IRS network in addition to providing e-mail access, increasing the risk that privacy and taxpayer data could be compromised. The IRS also allows devices based on the Android™ operating system to participate in the BYOD pilot, even though these devices are more subject to malware than the Apple® devices tested in earlier phases. Audit trails and training also need to be improved.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that a cost-benefit analysis for BYOD is completed that complies with Federal guidance, ensure that BYOD users are allowed access to e-mail functions only, takes some additional steps before admitting Android devices into the BYOD pilot, retains and reviews audit trails in compliance with existing policies, and provides periodic training for BYOD participants on threats and recommended security practices specific to BYOD.

In their response to the report, IRS management agreed with four of five recommendations and proposed some corrective actions that it plans to take only if the BYOD pilot is expanded or funding is identified. IRS management disagreed with the recommendation to defer admitting Android devices into the pilot until a security risk assessment is completed.

TIGTA believes that some of the corrective actions proposed by the IRS are inadequate because they are contingent on BYOD expansion or additional funding. The relevant controls should be put in place for the existing BYOD effort, which does not have a clear end date and which is being used by hundreds of employees and devices within the production environment.

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/201320108fr.pdf>