



Treasury Inspector General for Tax Administration Office of Audit

THE INTERNAL REVENUE SERVICE DOES NOT ADEQUATELY MANAGE INFORMATION TECHNOLOGY SECURITY RISK-BASED DECISIONS

Issued on September 22, 2014

Highlights

Highlights of Report Number: 2014-20-092 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Risk-based decisions are made when the IRS wants to make an exception to its own policies and requirements based on suitable justification and a thorough assessment of evident and potential risks. For decisions related to the security of information systems, exceptions are allowed if meeting the requirement is 1) not technically or operationally possible or 2) not cost effective. When risk-based decisions are not made within the established guidelines, the organization may be accepting too much risk related to security of its systems and data. Consequently, taxpayer data may not be secured and may be vulnerable to unauthorized disclosure, which can lead to identity theft. Furthermore, accepted weaknesses may result in security breaches, which can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquiries.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine whether the IRS's risk-based decision process provides an effective platform for identifying, assessing, and addressing risks related to information technology projects and systems. This audit is included in TIGTA's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The IRS collects and tracks minimal information about risk-based decisions and does not require supporting documentation about why decisions were made. In addition, information technology risks can be accepted and approved through different processes and may not be known by the Cybersecurity organization, which is responsible for the risk-based decision process. TIGTA also found that IRS risk-based decisions are not

adequately documented, and information about accepted risks is not centrally located.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) direct the Cybersecurity function to revise the risk-based decision policy and standard operating procedures to require complete information be collected for all decisions; 2) require all appropriate officials to be trained on what risk-based decision information is required, including justification for the decision based on either technical infeasibility or cost-effectiveness; 3) direct the Cybersecurity function to expand upon its current risk-based decision tracking efforts by maintaining supporting detail in a central repository; and 4) implement a quarterly review of risk-based decision detail to ensure compliance with existing IRS policy and to establish a foundation for risk management of information technology assets.

IRS officials agreed with our recommendations and plan to update policies to clearly state that risk-based decision justification information must be documented to include acceptance due to cost and technical limitations and will add these requirements to training materials. The IRS also plans to enhance the existing repository of risk-based decisions to maintain detailed justification information and will review this detail on a semiannual basis.

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/201420092fr.pdf>

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

Phone Number: 202-622-6500

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