



Treasury Inspector General for Tax Administration Office of Audit

AFFORDABLE CARE ACT: IMPROVEMENTS ARE NEEDED TO STRENGTHEN SECURITY AND TESTING CONTROLS FOR THE AFFORDABLE CARE ACT INFORMATION RETURNS PROJECT

Issued on September 29, 2014

Highlights

Highlights of Report Number: 2014-23-072 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

In March 2010, the President signed into law the Patient Protection and Affordable Care Act (ACA) to provide more Americans with access to affordable health care. The ACA Information Returns (AIR) Release 1 Project is an information technology project managed under the IRS's ACA Program. The ACA legislation requires the IRS to calculate and collect annual fees based on form reports provided by health insurance providers and pharmaceutical manufacturers and importers. The form reports include information that the IRS requires to calculate the fees that are due annually by September 30 of each year.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine if the IRS is adequately mitigating systems development risks for the AIR Release 1 Project. TIGTA evaluated the IRS's key management controls and processes for risk management, requirements and change management, testing, security, and fraud detection for the AIR Release 1 Project, which is being developed by following the IRS's Enterprise Life Cycle Commercial Off-the-Shelf Path.

WHAT TIGTA FOUND

The IRS conducted security activities to identify vulnerability weaknesses. The IRS also conducted testing activities to validate whether the AIR Release 1 system would function as designed before it was placed into production. However, improvements are needed to ensure the long-term success of the AIR system by adherence to systems development controls for security and testing activities in accordance with applicable guidance.

These security control weaknesses could impact the AIR system's ability to reliably process the electronic form reports and to accurately determine the applicable fees.

WHAT TIGTA RECOMMENDED

TIGTA's recommendations included that the Chief Technology Officer ensure that: (1) procedures are developed to provide direction on how to mitigate vulnerability weaknesses; (2) vulnerability weaknesses identified are promptly corrected and resolved; (3) the ACA Plan of Action and Milestones adequately addresses the vulnerability weaknesses within the required time frames; and (4) the Information Technology Implementation and Testing organization effectively manages the testing processes executed by the external contractors.

In management's response to the report, the IRS agreed with the majority of TIGTA's recommendations and plans to implement corrective actions. However, the IRS partially agreed with one recommendation and disagreed with two recommendations. TIGTA notes its concern about the IRS response to these recommendations in the report.

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/201423072fr.pdf>.