



Treasury Inspector General for Tax Administration Office of Audit

AFFORDABLE CARE ACT COVERAGE DATA REPOSITORY: RISKS WITH SYSTEMS DEVELOPMENT AND DEPLOYMENT

Issued on June 2, 2015

Highlights

Highlights of Report Number: 2015-23-041 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

In March 2010, the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act were enacted. These laws are collectively referred to as the Affordable Care Act (ACA). The ACA is intended to make health insurance more affordable and available to individuals. The IRS is developing the Coverage Data Repository (CDR) to help implement the ACA, and it will be the IRS's sole authoritative source of all ACA data for health care-related functions and services. During the 2015 Filing Season, the IRS will receive Exchange Periodic Data (EPD) from the Exchanges, store the EPD in the CDR, and use the EPD to verify the accuracy of the Premium Tax Credits claimed by taxpayers.

WHY TIGTA DID THE AUDIT

The overall objective was to determine how systems development risks for the CDR Project were being mitigated and whether established business and information technology requirements were being met. Specifically, TIGTA evaluated CDR testing processes, including interagency, release-level, and project-level functional testing controls as well as security and audit trail controls.

WHAT TIGTA FOUND

TIGTA found that risks could not be effectively mitigated by CDR testing processes. Interagency testing with the Federal and State Exchanges was not completed. As of November 21, 2014, the IRS had only received EPD from three States. Subsequent to our fieldwork, the IRS received additional data, but it still had not yet received all required EPD submissions from the Exchanges as of January 20, 2015, the start of the 2015 Filing Season.

Release-level testing was completed but not prior to initiating interagency testing with the Centers for Medicare and Medicaid Services. During project-level testing, system developers did not always demonstrate CDR functionality to business owners and did not

maintain complete records verifying business participation. The CDR was deployed before responsible officials completely assessed security risks and authorized the system to operate. The CDR Application Audit Plan was not implemented as needed to support the IRS's program and policy to mitigate risks for unauthorized access to taxpayers' records.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer 1) ensure that interagency testing with the Exchanges is completed, 2) ensure that future ACA projects complete release-level testing before starting interagency testing, 3) verify that CDR 2.0 functionality has been adequately demonstrated to ACA business owners, 4) ensure that sufficient evidence is maintained to verify adequate business owner participation, 5) ensure that authorizing officials evaluate and accept CDR risks prior to deployment, and 6) ensure that the CDR Application Audit Plan is completed, approved, sufficiently tested, and implemented.

In management's response to the report, the IRS agreed with two of TIGTA's recommendations. However, the IRS disagreed with three of TIGTA's recommendations and partially disagreed with a fourth. The Chief Technology Officer did not concur with recommendations to strengthen systems testing practices nor with TIGTA's assessment of the process applied to demonstrate and verify system functionality for the CDR. Because the IRS plans to rely on the CDR as its sole authoritative source for all ACA data, TIGTA maintains that improvements are needed to ensure adequate risk mitigation practices in each of these areas.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2015reports/201523041fr.pdf>

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

Phone Number: 202-622-6500

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