



Treasury Inspector General for Tax Administration Office of Audit

AFFORDABLE CARE ACT VERIFICATION SERVICE: SECURITY AND TESTING RISKS

Issued on September 28, 2015

Highlights

Highlights of Report Number: 2015-23-081 to the Internal Revenue Service Chief Technology Officer and Director, Services and Enforcement Affordable Care Act Office.

IMPACT ON TAXPAYERS

Starting with Tax Year 2014 individual income tax returns, the Affordable Care Act (ACA) requires taxpayers to file new forms (e.g., Form 8962, *Premium Tax Credit*, and Form 8965, *Health Coverage Exemptions*) to report that they have qualifying health care coverage, are eligible for a health coverage exemption, or make a shared responsibility payment. To process the new forms, the IRS developed the ACA Verification Service (AVS).

WHY TIGTA DID THE AUDIT

The overall objective was to determine if the IRS adequately developed and tested the AVS.

WHAT TIGTA FOUND

The ACA authorizing official signed the ACA security authorization, and the AVS was placed into production on January 20, 2015, prior to the completion of the security assessment. The authorizing official made this decision based on the results of security testing that had been completed, the Cybersecurity organization's memorandum concurring with the authorizing official's granting of an update to the current security authorization, and the urgent need to deploy ACA Release 5.0 at the start of the 2015 Filing Season. The Cybersecurity organization completed the security assessment in May 2015. AVS testing delays prevented the completion of security testing and the completion of documents needed for the security authorization package prior to deploying the AVS into production.

In addition, delays in testing extended the test period. Testing delays were caused by late code deliveries, changes in the test environment, and time needed to correct defects. Testing delays also caused numerous ACA builds, including the AVS, to be submitted for the Final Integration Test program approximately one week

before the start of the 2015 Filing Season, increasing the risk that defects would not be corrected prior to production.

Finally, test results from designated sources did not match the test results reported in the project-level and release-level draft End-of-Test Completion Reports. Discrepancies identified were due to clerical errors and the use of the Implementation and Testing organization's internal tracking system instead of only using the mandated tools.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief Technology Officer ensure that: 1) AVS security vulnerabilities are corrected prior to the next filing season; 2) security testing and security authorization packages are completed prior to authorizing and placing systems into production; 3) ACA developers are notified in advance when changes to the development, test, and production environments are made; and 4) testing organizations use only the information from the designated tools for documenting requirements, test results, and defects to prepare the End-of-Test Completion Report.

In their response to the report, IRS officials agreed with two of the four recommendations and partially agreed with the remaining two. For vulnerabilities that cannot be corrected prior to the next filing season, the IRS plans to continue following established procedures for addressing the vulnerabilities. When security testing and security authorization packages cannot be completed prior to system deployment, the IRS plans to exercise risk-based decisionmaking with appropriate governance approvals and documentation. IRS officials also stated that they have taken or plan to take appropriate corrective actions.

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/201523081fr.pdf>.