

Congress of the United States
Washington, DC 20515

December 6, 2013

The Honorable Daniel I. Werfel
Acting Commissioner, the Internal Revenue Service
U.S. Department of the Treasury
1111 Constitution Avenue, NW, Room 3241
Washington, DC 20224

Dear Commissioner Werfel:

Americans face a great threat to their personal security online, as it is widely understood that information systems can be hacked. Bad actors are constantly in search of opportunities to exploit vulnerabilities in our infrastructure, many of which are related to misconfigured system components and software flaws. Given this reality, we are concerned for the integrity and security of the sensitive personal data transmitted through the new health insurance exchanges. As you know, the Internal Revenue Service (IRS) is responsible for administering the premium tax credits (PTCs) established under the Affordable Care Act (ACA). Now that the health care exchanges are open for business, it is imperative that the IRS has processes in place to keep taxpayer information secure.

Recently, the Treasury Inspector General for Tax Administration (TIGTA) released a report that was completed on September 27, 2013 – days before the launch of the Healthcare.gov website. TIGTA determined that IRS has completed development and testing for the Premium Tax Credit Computation Engine (PTC-CE), which will calculate the PTC for eligible Americans. However, “critical” elements of the security controls failed during testing. Specifically, the report found that twelve controls were only partially implemented during the testing process. The ACA infrastructure components included in those twelve security controls also failed during the Security Controls Assessment, as they did not include the baseline configurations and mandatory configuration settings required by the National Institute of Standards (NIST) and Internal Revenue Manual (IRM) guidelines.

The report also found that Change Management Guidelines were not always adhered to when approved baseline security requirements were removed from the PTC Project. Just one of seven baseline requirements was removed from the PTC Project in accordance with the process outlined in the ACA Program Configuration Management Plan, which requires a change request (CR) and change impact assessment. The IRS’s IT Cybersecurity organization management stated that the organization does not have access to the CR Tracking System tool. Thus, it cannot ensure that CRs are approved, processed, and is “unaware of when final changes to the baseline security requirements were implemented.” This raises concerns as to whether the IRS can accurately determine how changed requirements will affect the security controls and operation of the PTC-CE.

TIGTA recommended that the IRS IT Cybersecurity organization resolve or develop a plan with specific corrective actions and time periods for the failed security tests that were reviewed as part of the ACA Security Assessment and Authorization. TIGTA states this resolution or action plan “is needed to ensure the IRS is addressing vulnerabilities in information systems that can be traced to software flaws and misconfigurations of system components for the PTC Project and across other information technology projects being developed” under the ACA.

We are also concerned that the TIGTA report indicates that during audit fieldwork, IT Cybersecurity organization officials “could not provide documentation to verify the corrective measures for the failed test controls.” According to the report, the IRS disagrees with the recommendation to develop an action plan and did not reference the audit findings that triggered the recommendation.

We find IRS’ refusal to adopt a corrective action plan of serious concern as the sensitive personal information of American taxpayers may be at risk. This audit raises important questions as to whether the IRS can successfully protect taxpayer data against fraud and abuse. Therefore, to better understand how the IRS plans to securely and successfully transmit taxpayer data, we respectfully request you provide a written explanation of the IRS’s process plan, along with copies of the documented policies for resolving the failed security tests. We also request an explanation on how the IRS coordinates with the ACA Program to ensure that change management guidelines are followed and that the PTC-CE operation is not impaired.

Thank you in advance for your attention to this letter. We look forward to your prompt reply.

Sincerely,



Patrick Meehan
Member of Congress



Diane Black
Member of Congress