

Congress of the United States
Washington, DC 20515

January 9, 2014

Mrs. Marilyn Tavenner
Administrator, Centers for Medicare & Medicaid Services
Department of Health and Human Services
Room 445-G, Hubert H. Humphrey Building
200 Independence Avenue SW
Washington, DC 20201

Dear Administrator Tavenner:

Cybersecurity threats to our government and private networks are among our nation's greatest security challenges. Rapid growth in technology creates an ongoing need to safeguard against new attacks, and bad actors seek to exploit vulnerabilities in our information systems. We are concerned for the security of HealthCare.gov, which processes the sensitive personal information of Americans – including, but not limited to their names, addresses, social security numbers, and residency status.

Developing an information system as complex as HealthCare.gov is a considerable endeavor that requires sufficient time to ensure the necessary controls that protect data systems are met. To this end, the Federal Information Security Management Act (FISMA) requires that federal information systems successfully complete security authorization in accordance with National Institute of Technology (NIST) standards. As part of this process, an authorizing official reviews the information needed to make a risk-based decision on whether to authorize operation of an information system, including the results of the Security Control Assessment (SCA). The authorizing official who signs the Authority to Operate certifies that all documentation has been reviewed and testing concludes that the system has met NIST guidelines.

On September 27, 2013, CMS issued an Interim Authority to Operate (IATO) authorizing the launch of HealthCare.gov. However, a risk decision memo that accompanied the authorization explained that the Security Control Assessment required by FISMA was only partly completed “due to systems readiness issues.” The IATO also appears to contradict regulatory guidance, which states that the Office of Management and Budget (OMB) does not recognize interim authority to operate for security authorization. Furthermore, reports that CMS' Chief Information Security Officer recommended a denial of HealthCare.gov's Authority to Operate are concerning.

Now that HealthCare.gov is open for business, it is imperative that Congress be provided the information necessary to understand how the federal exchange was certified and what

protections are in place to protect Americans using the system. What process has been implemented to monitor the ongoing effectiveness of security controls and the progress of actions taken to correct vulnerabilities? We respectfully ask that your office provide us with a copy of the SCA test that was to be completed within 60 to 90 days of launch, as outlined in the risk decision memo.

We also seek to understand who defined the controls that the system must adhere to, as directed by OMB, in addition to information detailing whether or not the controls were met, or were deemed deficient. In addition, we ask what additional security measures were considered when building the security of the network? Were the NIST standards the only guidelines used? Finally, we ask that you provide further clarification on the authority by which CMS may issue an IATO.

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