United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

October 29, 2013

The Honorable Kathleen Sebelius
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Sebelius:

As Members of the Committee on Finance (Committee), which has jurisdiction over implementation of the Patient Protection and Affordable Care Act (PPACA), we are seeking information about the various types of testing which were utilized to ensure that the healthcare.gov website and underlying system (hereinafter collectively referred to as "website") met all Federal privacy and security standards before going live on October 1, 2013. Additionally, we are requesting detailed information about security threats received since the website launch, as well as measures taken by your agency and contractors to ensure website security.

The Administration's Chief Technology Officer, Todd Park, publicly stated on September 11, 2013, that "after over two years of work, it [healthcare.gov] is built and ready for operation, and we have completed security testing and certification to operate."[1] Despite these and other assurances, we are troubled that day after day more issues arise which illustrate that the website was simply not ready to launch on October 1. While we recognize that the website's operational issues are being worked on and will likely be resolved eventually, serious questions remain as to the privacy and security of the very detailed personal information being transmitted through the Federally-Facilitated Marketplace (FFM) and what testing, if any, occurred or is occurring to ensure that information is secure.

It is our understanding that each Centers for Medicare & Medicaid Services (CMS) system is required by law to obtain an Authority to Operate (ATO) certification that attests the system has met all testing requirements before it is placed into operation. CMS' own internal procedures require that ". . . security controls be operational, effective, managed, and continuously monitored. Controls must meet mandatory requirements, as defined in the current CMS Information Security Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements (CMSR)."[2] Additionally, as the head of the Department of Health and Human Services (HHS), you are responsible for ensuring that your agency's information systems, including the website, fully comply with security requirements imposed by the Federal Information

[1] http://www.businessweek.com/news/2013-09-11/obamacare-computer-network-completes-security-tests-u-dot-s-dot-says.
[2] CMS Risk Management Handbook, Volume II, Procedure 7.8, August 17, 2012 (Document Number: CMS-CISO-2012-vII-pr7.8).

Security Management Act of 2002 (FISMA).[3] The website must also comply with the Office of Management and Budget's (OMB) implementing policies including Appendix III of OMB circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology.

To help us better understand how CMS ensured that these and other standards were met, please provide us with the following information:

- Describe in detail the security testing that was completed on all aspects of the healthcare.gov website before October 1, 2013. Please include copies of all testing certification or other documents that indicate the results of all testing that occurred.
- Please provide all timelines, dashboards or other tracking mechanisms developed to track the testing requirements.
- Was CMS/HHS granted a Privacy Act exemption by the Office of Management and Budget (OMB) for the website or any related applications? If so, please provide documentation for the exemption.
- Were any other security testing exemptions granted for the website or any related applications by OMB? If so, please provide all supporting documentation.
- Was all testing completed to meet the standards set forth by the FISMA? Please provide copies of all testing results and certifications that show all FISMA standards were met.
- Was a Privacy Impact Assessment (PIA) completed by CMS prior to the website going live? If so, please provide a copy of the PIA.
- Are reports generated on a regular basis regarding the security of the website and its related applications? How often are reports generated and what office (and whom) within CMS received those reports?
- What alerts are generated if an outside entity attempts to inappropriately gain access to sensitive information submitted to the website?
    - Since October 1, 2013, how many times has an outside entity attempted to inappropriately or unlawfully gain access to sensitive information?
    - Have any of these attempts been successful?
    - Provide a log of all alerts, or whatever method of tracking is used to track alerts, as well as the outcome of each alert (i.e., attempt was successful, not successful, etc.).
- Which contractors have access to user data submitted to the website?
    - How many employees at each contractor have access to this data?
- Provide names of the contractors that are responsible for staffing and operating all call centers associated with the website.
- With respect to each contractor retained by CMS to work on the website or the call center:
    - What measures are in place to ensure that these contractors appropriately secure data?
    - What training have these employees completed regarding how to handle sensitive data?
    - To date, have there been any instances when contractors have inappropriately disclosed or used data?
    - If so, what steps has CMS taken against the contractor and/or the employee?

[3] 44 U.S.C. § 3544.

- What security clearance is required for contractor employees who handle personally identifiable information (PII)?
    - Have all contractor employees been cleared to handle PII? If not, when does CMS anticipate that all employees will be cleared?
    - If any contractor employees are working with only a temporary clearance, what additional steps has CMS taken to ensure that these employees do not improperly disclose sensitive data?
- To your knowledge, have there been any improper disclosures of PII submitted by users of the website or the call center? If so, explain the circumstances and CMS' reaction.
- In the event that the website becomes no longer functional or suffers a loss of PII, does CMS have a disaster recovery plan? If so, please provide a copy of the plan.
- In the instances where a contractor who has access to personal identifiable information and is also owned by a company that participates in the exchange as a healthcare plan, what steps has CMS taken to ensure that personally identifiable information is not improperly provided to or used by the healthcare plan?

Wherever possible, please provide the information requested in electronic format. Thank you for your prompt attention to this request and we respectfully request receiving all information by no later than December 3, 2013. If you have any questions regarding this request please contact Kim Brandt of the Finance Committee staff at (202) 224-4515.

Sincerely,

Orrin G. Hatch

Charles E. Grassley

Mike Crapo

Pat Roberts

Michael B. Enzi

John Cornyn

John Thune

Richard Burr

Johnny Isakson

Rob Portman

Patrick J. Toomey