LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6301

(202) 225–6371
www.science.house.gov

December 11, 2013

President Barack Obama
The White House
1600 Pennsylvania Ave., N.W.
Washington, DC 20500

Dear Mr. President:

We write to request information and an explanation about what your Administration is doing to address the security risks and privacy concerns surrounding Healthcare.gov. During a teleconference with reporters on December 1, Mr. Jeffrey Zients, your National Economic Council Director-designate, stated that the Obamacare website is "night and day from where it was on October 1" and that the website can now "support intended volumes" of users.[1]

Though we appreciate the Administration's efforts to address the flaws with the website's capacity, we are concerned that the larger security and privacy issues remain unaddressed. While more people may be able to access the website, without much-needed security enhancements, this simply means that more Americans are vulnerable to online criminals and identity theft.

At a hearing before the House Committee on Science, Space, and Technology on November 19, leading computer security experts from the private sector and academia outlined the significant threats posed to Americans by identity theft. One witness, David Kennedy, is a so-called "white hat hacker" who helps private sector companies secure their websites and data from online criminals. Mr. Kennedy gave a demonstration of real vulnerabilities with Healthcare.gov, showing how hackers are attempting to access personal information on the website. According to his testimony, not only is the website vulnerable, it's under active attack. Even more troubling, Mr. Kennedy testified that there are "clear indicators that even basic security was not built into the Healthcare.gov website."

By design, Healthcare.gov interfaces with numerous federal, state and commercial sites and databases. The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. To gain information on

[1] CBSNEWS.COM Staff, "Healthcare.gov improvements 'night and day' from October launch," CBSNEWS.COM, December 1, 2013, available at: http://www.cbsnews.com/news/healthcaregov-improvements-night-and-day-from-october-launch/

potential healthcare coverage through the website, users must input personal contact information, birth dates and social security numbers, as well as income, tax and other intimate financial information.

Although the website itself does not retain personal data, it transmits it to other sites. Without adequate security measures, Healthcare.gov essentially becomes a portal for online criminals to access even more sensitive, personal data maintained by the IRS, state agencies, and insurance companies that share information with the website. The size and scope of information sharing alone raises significant security concerns.

When asked whether Healthcare.gov had been compromised by hackers, Mr. Kennedy testified that he believed the website already has been hacked or soon will be. Every single witness, majority and minority-invited alike, testified that Healthcare.gov is not secure. Asked if they would have launched the website, the unanimous answer was "No." Would they require front-end personal data disclosure on the site? Again, all four responded "No." Finally, each of the experts said taking down Healthcare.gov should be seriously considered to address the security concerns and protect the personal information of users. Mr. President, your Administration has an obligation to ensure that the personal, financial, and account information collected as part of the Affordable Care Act is secure.

Unfortunately, in its haste to launch the Healthcare.gov website, it appears that your Administration has cut corners that have left the website open to hackers and other online criminals. As a result, the personal information that has already been entered into Healthcare.gov is vulnerable to identity thieves. We already know of many attempts to hack into the system. If the security flaws go unaddressed, the more people who use the site will simply mean more Americans vulnerable to identity theft.

In light of the concerns of online security experts, the following questions need to be addressed to ensure the safety, security, and privacy of all Americans' personal data on the Obamacare website.

1) Since October 1, what explicit steps has the Administration taken to improve the security of Healthcare.gov?

2) Who in the Administration has been assigned to monitor, manage, and oversee the ongoing security needs of Healthcare.gov?

3) Has the Administration conducted thorough, on-going tests and monitoring of security and privacy vulnerabilities with Healthcare.gov—including hiring private sector "hackers" to test the website's ability to guard against malicious attack and intrusion? If so, who conducted the tests and on what dates? What were the operational details and specific results of these security tests?

Because of the seriousness of the threat facing users of Healthcare.gov, we ask that answers to these critical questions be provided to the Committee no later than December 18.

Sincerely,

Lamar Smith
Chairman

Rep. Dana Rohrabacher

Rep. Ralph M. Hall

Rep. F. James Sensenbrenner, Jr.

Rep. Frank D. Lucas

Rep. Randy Neugebauer

Rep. Michael T. McCaul

Rep. Paul C. Broun

Rep. Steven M. Palazzo

Rep. Mo Brooks

Rep. Randy Hultgren

Rep. Larry Bucshon

Rep. Steve Stockman

Rep. Bill Posey

Rep. Cynthia Lummis

Rep. David Schweikert

Rep. Thomas Massie

Rep. Kevin Cramer

Rep. Jim Bridenstine

Rep. Randy Weber

Rep. Chris Stewart

Rep. Chris Collins

cc: Rep. Eddie Bernice Johnson
Ranking Member