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

May 1, 2014

The Honorable Gene L. Dodaro
Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro,

As Chairman of the House Science, Space, and Technology Committee, I have held multiple hearings to examine concerns about the security of the Healthcare.gov website. The data obtained by Healthcare.gov is one of the largest collections of personal information ever assembled. It links information between seven different federal agencies and state agencies, as well as government contractors, making it a goldmine of Americans' personally identifiable information.

But in their rush to launch the website, the Obama Administration appears to have cut corners that have put the personal data of millions of Americans at risk. In addition to the website's initial security failings, many Americans now worry about how the Heartbleed Bug may compound the risk of financial or medical identity theft for those forced by the government to create Healthcare.gov accounts.

Security experts testified before the Science Committee that we need an accurate, independent, and impartial report on the security of Healthcare.gov. I agree.

I understand the U.S. Government Accountability Office (GAO) is currently conducting an audit of the security and privacy of Healthcare.gov that will include an architecture review, vulnerability testing, and an examination of the monitoring and incident detection capabilities of the website. However, I am concerned that the GAO does not plan to perform penetration testing, source code analysis, a review of the developer supply chain, or an examination of secure code practices through the software development lifecycle.

The American people deserve a thorough audit of the website to ensure that their personal data, including birth dates, social security numbers and household incomes, is protected. As the primary, non-partisan agency tasked with shedding light on government programs, GAO has a responsibility to conduct a full and thorough review of Healthcare.gov. This is one of the largest undertakings by the federal government in our nation's history—and the stakes are high to ensure that the website is secure.

Therefore, I request the following be conducted either as part of the current GAO audit, or as a separate audit that may supplement the current ongoing project:

1. Complete and continuous end-to-end testing, including full-scope penetration testing (exposing the system to internal and external hacking);
2. Source code analysis;
3. A full review of the developer supply chain to ensure that no unauthorized or malicious code, software, or hardware was introduced into the development or production environment, including by foreign nation state-sponsored activity;
4. Examination of the presence or absence of secure code practices through the software development lifecycle and the technology used to defend and protect against attackers; and
5. Determination of the specific involvement by staff of the Executive Office of the President relative to the development and implementation of the security and privacy standards of Healthcare.gov prior to October 1, 2013.

In conducting the audit, I encourage GAO to use outside security experts and private sector individuals, organizations, or companies that specialize in technical information security assessments that identify exposures through penetration testing and source code analysis; have a high competence and wealth of knowledge and experience as a core ability to perform these types of services; and are completely independent of people or firms that have an established relationship with the Healthcare.gov website and infrastructure.

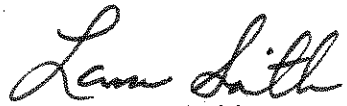
Upon completion of the audit, please provide the Committee with a determination by September 1, 2014, as to whether the Administration has effectively implemented appropriate controls to protect the confidentiality, integrity, and availability of the Healthcare.gov information systems and information. As part of that determination, please answer the following questions:

1. Is there higher than a low risk of security failure for any part of the Healthcare.gov system?
2. How, and in what timeframe, did the Incident Response Team handle the patch for the Heartbleed Bug? What assurances have been provided to verify the success of the patch?
3. Does the website meet or exceed generally accepted security best practices by employing leading edge standards and controls; employ a defense in-depth strategy that fully meets the standards recommended by the National Institute of Standards and Technology; and comply with the requirements and guidelines of the Federal Information Security Management Act?
4. Is there a Chief Information Security Officer in place who possesses the requisite responsibility and authority to provide continuous security testing, establish and implement proactive security controls and processes, and monitor the health and performance of the Healthcare.gov system?

5. Is the personally identifiable information elicited, collected, or stored in connection with the website, its infrastructure, and its data hub protected using security industry best practices, including Federal Information Processing Standards compliance with encryption, through the entire lifecycle of transmitting, storing, using, and processing personally identifiable information or sharing such information with other government agencies or third parties?
6. Has the website been designed and implemented with reasonable and demonstrable efforts to minimize domain name confusion, including through additional domain registrations and a program to educate consumers how to spot fraudulent websites?
7. Have proactive phishing detection and prevention capabilities been implemented and incorporated in the Healthcare.gov system?
8. Have all personnel who have access to personally identifiable information in connection with the website or with approving of services related to the obtaining of healthcare, including non-Federal personnel, favorably completed a background investigation, and if applicable, signed a nondisclosure agreement with respect to personally identifiable information?
9. Have proper precautions otherwise been taken to ensure that only trustworthy persons have access to personally identifiable and other sensitive information in the Healthcare.gov system?
10. Is there a formal, operational incident response team that reports to a Healthcare.gov Chief Information Security Officer with appropriate procedures in place for handling incidents that affect the safety and security of the Healthcare.gov system, including –
    a. continuous 24/7 monitoring and detection capabilities; and
    b. maintenance (either directly or through contract) of ample personnel to respond in a timely manner to incidents relating to the proper functioning and security of the website and to monitor on an ongoing basis existing and emerging security threats to the website?

I appreciate your cooperation with this initiative. If you have any questions, please feel free to have your staff contact Mr. Chris Wydler of the Committee at (202) 225-6371.

Sincerely,



Lamar Smith
Chairman

cc: Rep. Eddie Bernice Johnson
Ranking Member