

**U.S. House of Representatives
Committee on Science, Space, and Technology**

HEARING CHARTER

Is Your Data on the Healthcare.gov Site Secure?

Tuesday, November 19, 2013
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

At 10:00 a.m. on November 19, 2013, the Committee on Science, Space, and Technology will hold a hearing titled “*Is Your Data on the Healthcare.gov Site Secure?*” 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. In order to gain information on potential healthcare coverage through the website, users must input personal contact information, birth and social security numbers for all family members, as well as household salary and debt information. Users may also be asked to verify home mortgage and credit card information, place of employment, previous addresses, and whether the person has any physical and mental disabilities. This hearing will explore the threat posed by identity theft to Americans if hackers gained such information through the Healthcare.gov website, an assessment of the security controls in place and its vulnerabilities by cybersecurity experts not involved with the website, and what specific security standards and technical measures should be in place to protect Americans’ privacy and personal information on Healthcare.gov.

Witnesses

- **Mr. Morgan Wright**, Chief Executive Officer, Crowd Sourced Investigations, LLC
- **Dr. Fred Chang**, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University
- **Dr. Avi Rubin**, Director, Health and Medical Security Laboratory Technical Director, Information Security Institute, Johns Hopkins University (JHU)
- **Mr. David Kennedy**, Chief Executive Officer, TrustedSEC, LLC

Overview

The data on Healthcare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies¹ along with state agencies and government contractors. Federal agencies have a duty to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act (FISMA). However, according to documents from the Department of Health and Human Services, the security of the health care website had not been fully tested when it went public last month, and many cybersecurity experts have expressed concern about flaws in the website that put the personal data of Americans using the website at risk to identity theft from cybercriminals/hackers. According to testimony before the Homeland Security Committee, hackers have already tried to attack the Healthcare.gov website.²

Several government agencies within the Science, Space, and Technology Committee's jurisdiction have responsibilities with information security over the internet. According to the website of White House Office of Science and Technology Policy³,

The Obama administration and OSTP will develop policies that will:

- **Bring government into the 21st Century:** Establish a Chief Technology Officer position within the Executive Office of the President to ensure that every government branch and agency has the right infrastructure, policies and services for the 21st century
- **Create an Open and Transparent Democracy:** Develop cutting-edge technologies to create a new level of transparency, participation, and collaboration for America's citizens and enhance scientific integrity in government decision-making.
- **Protect America's Cyber Networks:** Initiation of new and powerful protection strategies to ensure that America's cyber network remains safe from espionage and disruption while at the same time increasing the Federal Trade Commission's enforcement budget so it can step up efforts to track down cyber criminals

Investment in these important technologies cannot be expected to remain strong if there is not an equally strong intellectual property regimen in place to promote innovation, investment and protect the rights of developers. And citizens cannot be expected to embrace these technologies unless they can be adequately assured that private information will be protected.

Under FISMA, the National Institute of Standards and Technology (NIST)—an agency within Department of Commerce—is tasked with providing standards and guidelines for non-Defense-related Federal agencies to use in developing Information Technology (IT) networks. The standards and guidelines that NIST issues require the Chief Information Officer (CIO) or Chief Technology Officer (“technology officer”) at each Federal agency to address certain privacy and security standards and document how those standards were applied or modified in the development, fielding and deployment of its IT network.

¹ The seven agencies are: Internal Revenue Service, Social Security Administration, Department of Homeland Security, Department of Defense, Department of Veterans Affairs, Office of Personnel Management and Peace Corps; See Stacy Cowley, “How Obamacare's 'privacy nightmare' database really works,” CNN.com, July 24, 2013, available at <http://money.cnn.com/2013/07/23/technology/security/obamacare-privacy>.

² <http://www.cnn.com/2013/11/13/politics/hackers-attack-obamacare-site/>

³ <http://www.whitehouse.gov/administration/eop/ostp/divisions/technology>

The first level of inquiry requires the technology officer to develop a system security plan. In developing such a plan, the technology officer must decide what level of security to provide. NIST guidelines provide assistance on the level of security that should be chosen as well as which security requirements correspond with each level. The guidelines outline specific controls that should be considered and the technology officer must consider each type of control and provide an explanation for choosing not to use certain controls.

The second level of inquiry is the information security risk assessment. Once the controls have been implemented, a security assessment should be performed based on NIST guidelines for the assessment of the security controls. The security assessment should determine whether the system and controls are operating as intended, whether the controls are implemented as intended, and whether the controls are supporting privacy policies. The technology officer then is required to provide a report assessing the security of the system.

The package accompanying the authorization to operate will include the security plan, the security assessment, and a plan of action and milestones. The plan of action and milestones are the future plans to continue addressing risk factors and continue monitoring risks. The technology officer for every Federal agency must decide whether to issue an authorization based on these three documents. An authorization to operate may be issued for up to three years, but may be for a shorter period time.

On September 3rd, shortly after an Inspector General IG report to the Center for Medicare and Medicaid Services (CMS) outlined concerns that CMS had missed several key deadlines and would not have time to adequately perform testing for the security of the website, the CMS Chief Information Officer supported moving forward with approval of the website despite indications of numerous issues that could compromise its security. The documents indicate that the system security utilizing the NIST guidelines was identified as a Moderate level rather than a High level.

In addition to the threat from hackers with malicious intent of identity theft, the Healthcare.gov system is also routing personal information about individuals to the wrong people. According to news reports, Mr. Justin Hadley of North Carolina recently downloaded a letter from the Healthcare.gov website that included personal information belonging to Mr. Thomas Dougall of South Carolina. Mr. Dougall contacted the website to rectify the problem, but soon realized they had “no procedure whatsoever to handle security breaches.”⁴ Another case involves a Missouri woman, Ms. Lisa Martinson, who called Healthcare.gov’s customer service after forgetting her password. She was informed that three different people were given access to her account, address and social security number and that “it would take up to five days to get her personal information offline.”⁵

⁴ Sterling Beard, “Healthcare.gov Users Warn of Compromised Personal Information,” *National Review Online*, Nov. 4, 2013, available at <http://www.nationalreview.com/corner/363031/healthcaregov-users-warn-compromised-personal-information-sterling-beard>.

⁵ “Missouri woman's personal information stolen from Obamacare website,” *Examiner.com*, Nov. 9, 2013, available at: <http://www.examiner.com/article/missouri-woman-s-personal-information-stolen-from-obamacare-website>.

The focus of this hearing will be the threat posed by identity theft to Americans if hackers with malicious intent gained such information through the Healthcare.gov website, an assessment of the security controls in place and its vulnerabilities, and what specific security standards and technical measures should be in place to protect Americans' privacy and personal information on Healthcare.gov.