Written by **Michael Tennant** on January 17, 2014

ObamaCare Website Still Not Secure, Experts Tell House Panel

Security experts have long warned of major vulnerabilities in Healthcare.gov, the federal ObamaCare exchange website, but "there has been little effort to address [these] concerns," one such expert told the House Committee on Science, Space, and Technology Thursday. Meanwhile, he said, researchers continue to identify new vulnerabilities in the website.

"The consistent feedback that we got was that Healthcare.gov is not secured today, and nothing's really changed since the Nov. 19 testimony," said David Kennedy, CEO and founder of Ohio-based information-security firm TrustedSec. "In fact, from our Nov. 19 testimony, it's even worse."

Of the 18 issues identified during that November hearing, Kennedy stated in written testimony that only "a half of one issue" had been "fixed." Other critical issues remain, while new ones "have been identified and reported" but "have not been fixed," he added. "One of the more alarming is the ability to access anyone's eligibility reports on the website without the need for any authentication or authorization."

Healthcare.gov "fails to meet even basic security practices for protecting sensitive information of individuals and does not provide adequate levels of protection for the website itself," he said.

What's more, Kennedy observed, much of this was known prior to the website's launch, but the Obama administration chose to proceed with it anyway. "The website ultimately went live on Oct. 1 without ever having undergone complete end-to-end-security testing," ABC News reported. Centers for Medicare and Medicaid Services chief information security officer Teresa Fryer told the House Oversight Committee in December that she notified three high-ranking officials at the Department of Health and Human Services of the serious risks she believed to be inherent in the website prior to its launch; but her concerns, while acknowledged, were ignored.

Documents from the House Energy and Commerce Committee show that "monitoring and detection capabilities hadn't even been created or started prior to the launch of the healthcare.gov web site, and had not started by November 19th, 2013," Kennedy testified.

The administration seems not to be particularly concerned with security even now. Although the original website contractor, CGI, has been replaced by a new contractor, Accenture, that new contractor is hardly an improvement when it comes to security. "Accenture also developed the California state exchange, which has significantly more exposures currently than the healthcare.gov web site," Kennedy said, including "the ability [for a hacker to] extract over 500,000 user's [sic] personal information."

Kennedy was not alone in his assessment of the ObamaCare website's security flaws.

"The Healthcare.gov website is a major target for hackers who are looking to steal personal identities," Michael Gregg, CEO of Texas-based security-assessment firm Superior Solutions, told the committee in written testimony. "A successful attack against HealthCare.gov … could very well be the largest [such attack] ever."

Gregg is skeptical of the website's security in large part because of the size of the site and the rapidity with which it was developed and deployed:

> HealthCare.gov is reported to be about 500 million lines of code…. Windows 8 is reported to be no more than 80 million lines of code. Microsoft has spent almost 30 years attempting to secure their operating systems. It's illogical to believe such a large site such as HealthCare.gov, could be secured in such a short period of time. To believe that this has occurred would mean that the contractors responsible for the development of this site have been able to do what no other major company … has ever accomplished.

He is also concerned, he said, because the website is reportedly "only being scanned and patched after problems are discovered." By then, of course, hackers could have already obtained the data they want. "Think of it in this way," Gregg explained. "The site administrator must find and secure all problems yet a hacker only needs to find one vulnerability to exploit the site."

Why would hackers be interested in Healthcare.gov? Traditional identity theft is one obvious reason. Another reason is *medical* identity theft. "Such attacks are on the rise," Gregg said. "A study by the Ponemon Institute found that a whopping 94 percent of polled healthcare organizations have suffered 'data breaches' that exposed patient records…. A 2012 report from the U.S. Department of Health's Office of Civil Rights … found that in just three years nearly 21 million patients became the victims of medical record data breaches."

Americans are all too familiar with the consequences of identity theft, but what can one expect if his medical identity is stolen? Gregg listed a few possible scenarios: "not getting hired for a job," "getting the wrong treatment," and being "denied life insurance."

Although no successful attacks on Healthcare.gov are known to have occurred thus far, this does not mean the site is safe, Gregg argued. Hackers may simply be biding their time, waiting for more people to enroll in ObamaCare, so that they can obtain even more personal data before their attacks are detected and thwarted, he said.

Kennedy, Gregg, and other experts who testified recommended major changes in the security practices surrounding Healthcare.gov, not least of which is hiring an independent third party to review the current practices and recommend improvements.

Kennedy further suggested that the problem is not confined to Healthcare.gov but is a government-wide issue. "The lack of formal security testing and proactive security measures to which to adhere in the federal government is alarming," he said, adding that "immediate action must be taken in the federal government to protect sensitive information and remain competitive with other nations."