



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

**Opening Statement**

November 13, 2013

**Media Contact:** Charlotte Sellmyer  
(202) 226-8417

---

**Statement of Chairman Michael McCaul (R-Texas)  
Committee on Homeland Security**

**“Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed  
Healthcare.gov?”**

This hearing is part of our ongoing oversight of the rollout of the Patient Protection and Affordable Care Act, also known as Obamacare.

Today’s hearing follows two subcommittee hearings held by Chairman Pat Meehan on the security of the data hub and healthcare exchanges. I would note that in those two hearings, the Centers for Medicare and Medicaid Services (CMS) repeatedly assured this committee that the systems would be both functional and secure. Those assurances ring hollow in light of the disastrous rollout of Healthcare.gov. We are concerned that the security of the system is as flawed as its functionality.

The Department of Homeland Security (DHS) has two roles in the implementation of Obamacare. The first is to verify the immigration status of applicants, and we look forward to hearing more about how this system works from Ms. Correa of U.S. Customs and Immigration Services (USCIS) who is here with us today.

The second role DHS plays in Obamacare is overseeing the security of federal civilian networks. According to the Department’s website, “DHS is responsible for overseeing the protection of the .gov domain.” That being the case, I think it would surprise many Americans to know that DHS had effectively no input into the security of Healthcare.gov, despite it being arguably the most significant federal government website ever constructed.

To be clear, DHS has not participated in any meaningful way in developing, monitoring or ensuring the security of Healthcare.gov, the Health Exchanges or the Federal Data Services Hub. The only contact between DHS and CMS consisted of two emails and one phone call.

Departments and Agencies are responsible for setting up their own cybersecurity systems but because of statutory limitations, DHS can only recommend policies and offer assistance on a voluntary basis. In this case, CMS never asked DHS for advice, technical assistance or even a threat briefing.

It is with this limited oversight that the same people at CMS who told us the system would work are telling us it is secure.

The reason this concerns me is that if consumers are able to log on to Healthcare.gov, they are required to enter vast amounts of personally identifiable information about themselves and their family members. This information includes their name, addresses, date of birth, social security number, citizenship and immigration status, employer information, veteran status, household income, requests for religious exemption, current health status such as whether or not the applicant is pregnant or has a disability, among other things.

While the Administration and some of my colleagues across the aisle point out that the data services hub does not store this information, it is important to note that the state exchanges, and the federal exchange servicing 34 states, store and keep that information for up to 10 years.

All of this information is a tempting target for hackers, identity thieves and other malicious actors. We already have reported cases of hacks, fraudulent websites and documented security vulnerabilities in the system. We are also concerned that the so-called "Navigators," charged with helping people enroll in Obamacare, are not subjected to background checks. This will undoubtedly result in cases of fraud and identity theft, most of which we won't even know about for months. In fact, just yesterday we received reports of Navigators in my home state of Texas encouraging applicants to lie in order to get higher insurance subsidies.

Even if a system worked properly, the centralization of so much personal data would create security concerns. But in this case, Healthcare.gov is so flawed those concerns are even greater. Mr. Luke Chung will testify today to shed some light on the technical problems with Healthcare.gov and how those affect security.

Moving forward, we believe it is vital for the federal government to use every asset it has, including DHS, to secure its networks and ensure the security of Americans' most sensitive personal data.

As such, DHS needs to have not just the responsibility, but more importantly the tools and authorities it needs to secure the .gov domain. Our committee is currently working on legislation to address this by codifying the DHS cyber mission. We look forward to working with the Ranking Member and other Members of the Committee as we move that bill through the legislative process.

###