



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

*Opening Statement*

July 17, 2013

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

---

**Statement of Subcommittee Chairman Patrick Meehan (R-PA)  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies  
Committee on Homeland Security**

*Joint Subcommittee Hearing with*  
**Subcommittee on Energy Policy, Health Care and Entitlements  
Committee on Oversight and Government Reform**

**“Evaluating Privacy, Security, and Fraud Concerns with ObcamaCare’s Information Sharing  
Apparatus”**

**July 17, 2013  
Remarks as Prepared**

This hearing comes at a critical time in implementing one of the key aspects of the President’s healthcare law, the federal data hub. It is not my intention to relitigate the Affordable Care Act at today’s hearing, but rather to provide crucial oversight over the government’s establishment of the federal data hub. As a result of the Affordable Care Act, the Department of Health and Human Services is building an enormous data-sharing network between state health insurance exchanges and numerous federal agencies. The purpose of the data sharing hub is for the government to determine whether Americans who enter the exchange are eligible to do so.

As Chairman of the House Homeland Security Committee’s Cybersecurity Subcommittee, we have looked extensively at the access to and management of Americans’ personally identifiable information by the Federal Government.

I don’t need to explain to this committee, to our witnesses, or to the American public from where our concerns emanate. We have witnessed all too recently how sensitive information can be mismanaged by the Federal Government. We have seen how cyber attacks from adversarial nations who seek to infiltrate our country’s military and intelligence information have breached our most secure networks. We have watched as thieves have stolen our top innovators’ intellectual property. We have witnessed American financial service institutions succumb to barrages of attacks by those who wish to do our nation and our way of life harm.

FBI Director Robert Mueller has said that “the cyber threat...will be the number one threat to the country.”

NSA Director General Keith Alexander called the loss of intellectual property through cyber espionage, “the greatest transfer of wealth in history.”

Former Secretary of Defense Leon Panetta said that cyber attacks could soon shift from “espionage to destruction.”

The Director of National Intelligence General James Clapper has said that “potentially disruptive and even lethal technology” continues to become easier to access. And that “we foresee a cyber-environment in which emerging technologies are developed and implemented before security responses can be put in place.”

Former FBI Director Louis Freeh just recently said that our nation’s transportation systems, aviation guidance systems, highway safety systems, and maritime operations systems are all vulnerable to an attack.

These are serious people, who have been charged with securing the most critical data in the world. Although, one could certainly make the argument that the personally identifiable information of millions of Americans are even more critical to our nation than national security data.

Javelin Strategy and Research found that 12.6 million Americans are victims of identity theft each year.

A February 2013 study by the Center for Strategic and International Studies found that 85 per cent of government and private sector network breaches took months to be discovered.

PricewaterhouseCoopers estimates that one third of those breaches come from employees.

With over twenty million Americans estimated to enter into the exchange over the next five years, this leads to the question, which I believe must be answered at today’s hearing: are you ready?

Does CMS have the tools in place to secure the information of over 20 million Americans?

Who and how many will have access to this information? How do we ensure competence in those that have access?

I have grave concerns about the ability to establish sufficient security in this massive, unprecedented network by October 1st, when our most secure networks are breached every day. Every sector, every agency, every industry concerned with security will tell you that they are only as strong as the weakest link.

I hope that our panel today can allay some of these concerns. But I fear that our government is about to embark on an overwhelming task that will at best carry an unfathomable price tag, and at worst place targets on every American who enters the exchange.

###