



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

April 25, 2013

Media Contacts: Mike Rosen, 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**

“Striking the Right Balance: Protecting Our Nation’s Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties”

**April 25, 2013
Remarks as Prepared**

I would like to welcome everyone to today’s hearing, “Striking the Right Balance: Protecting Our Nation’s Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties.”

During this Congress, our subcommittee has been examining the cybersecurity threat to individuals and to our critical infrastructure. Our nation has made great strides, but the threat is multifaceted, and we are only as strong as our weakest link. Earlier this week, we saw the ramifications of a hacked twitter account that nearly sent our financial markets into a tailspin. While the Dow Jones industrial average recouped its losses, the lesson is clear: we are in an interconnected world, and a successful attack on one network will certainly impact others.

The Department of Homeland Security plays a crucial role in preventing cyber attacks on our government and critical infrastructure key resources.

As Chairman McCaul and I continue our efforts to craft legislation to bolster existing structures and improve the capabilities at the Department of Homeland Security, one of the key challenges will be to strike that balance of securing our networks and ensuring protections for our citizens.

Upon assuming the gavel of this subcommittee this year, I made sure that I immediately reached out to leading privacy advocates. Groups like the American Civil Liberties Union and the Center for Democracy and Technology have been instrumental in shaping our committee’s work.

Indeed, we must make clear that the purpose of sharing information is to prevent a cyber attack, and nothing else. Any intelligence shared with the government or with private entities must include protections for consumers and individuals.

In order to accomplish this, we must ensure that we have a full understanding of:

- what the threat is;
- what type of intelligence is necessary to share to prevent an attack;
- what type of information is inadvertently caught in the net;
- and furthermore, what is done with it once identified.

The answers to these questions coupled with robust civilian oversight, a clear set of rules of conduct, and liability protections for those acting in good faith, will help shape the key policy initiatives for our subcommittee.

Our committee is not concerned with the internet habits of ordinary Americans. And it is our duty, as members of this committee to make sure that the Department does not monitor, collect, or store the online activity of law-abiding American citizens.

Therefore, information that permits the identity of the individual to be directly or indirectly inferred, also referred to as “Personally Identifiable Information” must be protected.

DHS has significant inherent advantages that enable the Department to facilitate communications among the sixteen critical infrastructure sectors. The Department of Homeland Security Privacy Office is the first statutorily-required privacy office in any federal agency. The office is responsible for evaluating Department operations for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact.

By employing the Fair Information Practice Principles, or “FIPPs”, the DHS Privacy Office is charged with ensuring that the Department’s data collection methods are transparent, have specified purposes, and include data minimization, use limitation, data quality and integrity, security, and accountability and auditing.

It is for these reasons that many intelligence and cybersecurity experts point to DHS as manning a significant role in combating the threat. In fact, the Director of the National Security Agency, General Keith Alexander has said that due to the Department’s transparency, he sees “DHS as the entry point for working with industry.”

Building our nation’s capacity to prevent cyber attacks is as complex as it is essential. As a former U.S. Attorney, I can tell you that the Department of Justice has a very important role to play in enforcing our cyber crimes laws. We also must permit our military and foreign intelligence capabilities the resources to protect our nation’s defense. And equally as important, the Department of Homeland Security has the mission of defending our nation’s key resources and the liberties guaranteed in our Constitution.

We have an excellent panel of witnesses today, who will help us answer these questions, and hopefully help us find the balance. Moving forward, today’s hearing aims to examine how DHS currently protects privacy and personally identifiable information, address the legitimate privacy concerns that are inherent in sharing cybersecurity threat information, and find ways to strike that proper balance between privacy and security.

No one should mistake the common cause of securing our homeland for authority to violate the civil liberties of Americans.

###