



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

February 25, 2015

Media Contact: April Ward
(202) 226-8477

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

“Examining the President’s Cybersecurity Information Sharing Proposal”

Remarks as Delivered

At the dawn of the digital age, our nation saw endless opportunities to generate prosperity by expanding our networks and connecting to the world. But today, American prosperity depends as much on defending those networks as it does on expanding them.

Every day our country faces digital intrusions from criminals, hackers, terrorists, and nation-states like Russia, China and Iran. The impacts of those intrusions are felt everywhere—from our national security secrets to the personal information of Americans.

We cannot tolerate acts of cyber vandalism, cyber theft, and cyber warfare especially when they put our nation’s critical infrastructure at risk and when they steal American intellectual property and innovation. Accordingly, our government must play a leading role in combating threats in the digital domain.

It is clear that safeguarding American cyberspace is one of the great national security challenges of our time. We are confronted almost daily with frightening new precedents, such as the North Korean cyber attack on Sony Pictures—a cowardly act meant to intimidate Americans and stifle freedom of expression.

This attack came from a nation-state using a digital bomb to target and destroy computer systems here in the United States. Iranian-backed hackers also demonstrated this capability when they attacked Saudi Arabia’s national oil company, Aramco, and destroyed 30,000 computers. Iran also continues to target major U.S. banks to shut down websites and restrict Americans ability to access their bank accounts.

Imagine this type of attack on our gas pipelines or power grid in the Northeast. Such assaults on our critical infrastructure could cripple our economy and weaken our ability to defend the United States. These scenarios sometimes sound alarmist, but we must take them seriously as they grow more realistic

every day. Our adversaries are hard at work developing and refining cyber attack capabilities, and they are using them to intimidate our government and threaten our people in both times of peace and times of conflict.

But the threat extends beyond the industrial engines that drive our economy to the homes of Americans themselves. Criminals and countries alike can use cyber attacks to raid Americans' savings accounts or steal their personal health records.

The recent breach of health insurer, Anthem, illustrates the intrusiveness of these attacks. That assault alone exposed the personal information of up to 80 million people, including the names, birth dates, and social security numbers of tens of millions of children. But this is just the latest in a long string of cyber breaches targeting private citizens—a list that includes breaches at Target, Neiman Marcus, Home Depot, and JP Morgan.

Our adversaries are also seeking to steal secrets from our government and our most innovative companies. We know that Chinese hackers, for instance, continue to breach federal networks for the purpose of espionage and attack major U.S. businesses to give themselves a competitive edge in the global economy. Make no mistake: these attacks are costing Americans their time, money, and jobs. General Keith Alexander has described cyber espionage and the loss of American intellectual property as the “greatest transfer of wealth in history.”

Sadly, our laws are not keeping up with the threat. For instance, fearing legal liability, many private companies choose to not disclose the threats they see on their own networks, leaving others vulnerable to the same intrusions.

We cannot leave the American people and our businesses to fend for themselves. Now, more than ever, Congress must take aggressive action.

This year I will lead a renewed effort to push cybersecurity legislation through Congress. Last year, the ranking member and I, and this committee, passed five cyber bills. These new statutes lay out the rules of the road on how cyber information will be shared between government and the private sector so that the two can work together to combat this persistent threat. The laws also provide important protections to ensure Americans' information and civil liberties are not compromised.

But now, we must build on that success. And, we can start by creating a “safe harbor” where legal barriers to sharing cyber threat information are removed and the private sector is encouraged to collaborate. This will allow us to respond to cyber incidents more quickly and effectively—and will give government and private entities the ability to see the threat landscape in real-time.

I am pleased the president has come forward with a proposal on this important issue. Our solutions must transcend partisan boundaries if we are going to tackle this challenge. The American people are counting on us.

I want to thank the witnesses for testifying before this committee and I look forward to your testimony.

###