Opening Remarks: Open Cyber Threats Hearing

February 14, 2013

Thank you, Mr. Chairman.

Last year at this time, I warned of a cyber cold war. In 2012, we saw the cyber war turn hot.

Less than a month ago, both the New York Times and the Wall Street Journal reported that Chinese hackers attacked their systems over the course of months and infiltrated their computers.

According to the Security firms they hired, the Chinese Government itself was behind this attack.

Earlier in 2012, media reports said that a group from Iran was behind a series of major computer attacks against a large oil company, Aramco. The malicious code devastated over 30,000 computers!

Hackers also have been targeting our Government systems.

One group recently hijacked the website of the U.S. Sentencing Commission, the agency responsible for our federal sentencing guidelines.

In 2012, this Committee issued a report demonstrating the threat that certain foreign electronic companies pose to our mobile phones, our computers and our critical Government systems.

Every day, and as we speak, our Government and private sector companies are under attack. Nations are trying to steal our military and intelligence secrets, as well as our companies' most valuable trade secrets, threating U.S. profits and American jobs.

They are trying to steal our financial information, and our most private health records.

Cyberspace has become where the most business activity and development of new ideas takes place, and it will continue to do so. Cyberspace is where America will lead the next generation of innovation.

Cyberspace is America's virtual land of opportunity.

But it is also the land most vulnerable to bad activity. Private hackers and foreign intelligence services are trying to exploit this vulnerability every day. The more "wired" we become, the more efficient and productive we become, but also the more at risk.

So, we must fully understand this threat, and we must do everything we can to defend against it. We need to understand our vulnerabilities and always remain vigilant.

We already know that neither private industry nor the Government can solve this problem alone. We know we need to share threat information with industry, and that industry has to share threat information with the Government. We know we need to remove the barriers to information sharing.

Two nights ago, in his State of the Union address, President Obama agreed with us on the need for legislation. His Executive Order is a very good step, and it helps clear the way for the successful passage of a cybersecurity bill. By providing critical infrastructure protections, the Executive Order can help break the impasse in the Senate over this issue.

No Executive Order, however, can enable information sharing from private industry to Government, because it cannot provide the liability protections companies need before they will share threat information. Our bill recognizes that if one company is under attack, it will not tell the Government if it fears being sued for doing so.

Our bill also recognizes that only companies that act in good faith should receive this liability protection.

We know we need cyber legislation for the 21st century, and we know we need it now.

We also know that individuals need to do their part—whether using passwords more sophisticated than the name of their pets, to being wise against on-line scams and keeping anti-virus software up-to-date.

Cybersecurity is national security. All of us need to do our part. And, fortunately, we have extremely capable and dedicated public servants who have devoted their lives to keeping us safe. Governor Engler, Mr. DeFontes, Mr. Smocer, and Mr. Mandia, thank you so much for being here today. We greatly appreciate all the work you and your agencies are doing on our behalf, and I look forward to your remarks.

Mr. Chairman, I yield back.