

ONE HUNDRED TWELFTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

Opening Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
Hearing on “Cybersecurity: Threats to Communications Networks and
Public-Sector Responses”
Subcommittee on Communications and Technology
March 28, 2012

Thank you, Mr. Chairman, for holding this hearing on cybersecurity. It is important that we understand the government perspective. I am especially interested to learn the steps government agencies are taking to advance cybersecurity and secure the supply chain. I also welcome our expert from Carnegie Mellon.

The FCC, under the leadership of Chairman Genachowski and Admiral Barnett, has established a Communications Security, Reliability and Interoperability Council, or “CSRIC”. Today, we can learn about CSRIC’s recent recommendations promoting cybersecurity, as well as what other agencies are doing to promote best practices and information sharing.

Efforts like CSRIC can help lead to adoption of best practices and voluntary codes of conduct by internet service providers, software companies, manufacturers, and security vendors. But we also need to address the question of accountability. For example, what if one company fails to be as diligent as others in following best practices and, as a result, causes a cyber breach that rises to the level of a national concern? We need to explore whether reliance solely upon the private sector to ensure the security of communications networks across the country is sufficient, and what additional steps we might need to achieve enough accountability to best protect critical communications networks from cyber attacks.

We are hearing from industry that they want statutory exemptions from privacy and antitrust laws in order to facilitate information sharing. I have an open mind as we consider these issues. But this should be a two-way street. If industry wants exemptions from consumer protection laws, we have a right to ask for accountability that companies actually end up sharing information important for cybersecurity, do not abuse their privileges, and are held accountable.

There is a stronger case to be made for enabling sharing between the federal government and private industry. But we need to balance information sharing with sufficient privacy and civil liberties protections.

Further, we need to make sure that the federal agencies that engage in direct information sharing with the private sector are civilian agencies, not intelligence or defense agencies.

I hope we will also discuss securing the communications supply chain. This is a growing potential threat, especially as we are now witnessing thousands of applications being loaded onto smart devices that connect to the public Internet. We should examine the best ways to address this.

Thank you to our panel of witnesses for your participation today. I look forward to hearing your testimony.