

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. Diana DeGette
Ranking Member, Subcommittee on Oversight and Investigations
Hearing on “Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security”
Subcommittee on Oversight and Investigations
February 28, 2012

Thank you, Mr. Chairman, for holding this hearing on smart grid cyber security. Last year, in July, the Department of Homeland Security came before this Subcommittee to discuss their efforts to protect and deploy federal resources and to coordinate with the private sector to prevent and respond to cyber attacks. Today’s hearing is an important follow-up.

Protecting our critical infrastructure from cyber attacks is of vital importance. As our electrical grid evolves, we become more and more dependent on “smart” technologies to control, connect, and maintain this interconnected system. This is a good thing – it will make the grid more efficient and more reliable. For example, customers will soon be able to track the price of electricity minute-by-minute and adjust electricity use accordingly - waiting until prices are right to do the laundry or start the dishwasher.

However, these investments also expose us to new threats. These new technologies can be easy prey for hackers or terrorists who seek to bring down unprotected networks. As the smart grid becomes more interoperable, these attacks could have debilitating effects nationwide. In 2007, DHS ran a test, known as Aurora, which showcases just how dangerous grid vulnerabilities can be. They used a dial-up modem to rewrite computer code and remotely detonate an industrial-control-system generator.

That is why I’m pleased we are having this hearing today. We, as a Congress, must do everything in our power to ensure that the grid remains safe and secure. The testimony we hear today will help us understand our successes and identify flaws in the current approach so we can understand what else can be done to protect the smart grid. This hearing will also help us understand if Congress needs to provide more resources or more legislative authority for key cybersecurity agencies.

The Administration has made cybersecurity a priority – launching a Comprehensive National Cybersecurity Initiative to protect the digital infrastructure. The President’s FY2013 budget includes \$769 million to support the National Cybersecurity Division within the Department of Homeland Security. These funds are targeted at improving monitoring on federal networks to respond to cyber threats, and supporting cyber attack responses for critical

infrastructure owners and operators and for state and local authorities. I commend this targeted focus on cyber security. But I am hoping that today we can learn more about any gaps in security that may still exist.

Mr. Chairman, I appreciate that you are holding this hearing, and hope you will continue to look for other areas where we can work together in a bipartisan fashion. And, as we hear from our witnesses today, I hope we do not forget that the issue of cybersecurity goes well beyond the protection of our critical infrastructure. Consumers entrust important personal information to their banks, their internet service providers, their credit card companies, and the retailers from whom they purchase items online.

These companies should ensure they are protecting this information – and Congress needs to be doing its oversight job to verify that this is the case.

Yet, every day, we hear a new story about e-mail accounts being hacked, credit card information being hijacked, and social security numbers or other important personal information being stolen by cyber criminals. The loss of this information can be costly and personally damaging. In September of last year, the internet security company Symantec issued the Norton Cybercrime Report and calculated that cyber crime costs companies and consumers \$114 billion annually. That same report found that more than two thirds of adults online had been the victims of a cyber crime.

As our use of internet services become more and more integrated – using the same internet services for email, social networking, photo sharing, bill paying, and browsing and search – we have to be more vigilant in ensuring the protection of our personal information. Sites like Google, Yahoo and Facebook will be targets for hackers, and if successful, these cyber attacks will have a major impact on the American public.

For that reason, Mr. Chairman, in addition to investigating how the government can improve critical infrastructure cybersecurity, this Subcommittee should also look closely at what the private sector is doing to prevent cyber attacks and keep consumers' personal information safe.

I am pleased to see our continued focus on this issue – and hope that as the year goes on, we can hold more bipartisan hearings like this, focusing on both the government and the private sector role in protecting our critical infrastructure and our personal information from cyber criminals.