<u>OPENING STATEMENT</u>

Ranking Member Daniel Lipinski (D-IL)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
Subcommittee on Oversight
"Cyber Security: What the Federal Government Can Learn from the Private Sector"
January 8, 2016

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on cybersecurity. I want to thank all the witnesses for being here today and I look forward to hearing your testimony.

I am pleased that our first hearing of the year is on cybersecurity, an increasingly urgent challenge for our national security and the personal security of every American. It is important that we continue to hear from experts in government and the private sector about the latest developments with respect to both the risks that confront security in cyberspace, and the technologies and policies to combat those threats. Our Committee plays an important role in both the technology side and the policy side, and this is an area in which Members have successfully collaborated across the aisle. In December 2014, Congress enacted the *Cybersecurity Enhancement Act*, a bipartisan research, education, and standards bill that I worked on with Mr. McCaul over several years. And last month Congress enacted a cybersecurity law to promote information sharing and strengthen coordination between the private and public sectors. As a Committee and a Congress we need to continue to confront these serious cyber threats.

Unfortunately, we continue to see an increase in major cyber-attacks in both the public and private sectors. In a hearing we held here in July, we heard about the significant breach at the Office of Personnel Management (OPM), in which the personal information of millions of current and former federal employees and job applicants was compromised. Highly sensitive security-clearance files were compromised, making it not just a problem for all those individuals but a national security issue as well.

We have laws in place to address the security of federal information systems. The Federal Information Security Management Act, or FISMA, and subsequent amendments establish the necessary policies and procedures for the development of standards and protocols;

NIST has an important role in this. But it is clear that federal agencies need to do a better job implementing NIST's standards and protocols, and that Congress needs to give them adequate resources to do so.

The private sector is also under constant threat from cyberattacks. In the case of large-size companies, a recent study conducted by the Ponemon Institute found that there was a 19 percent increase in cybercrimes between 2014 and 2015. The study also found that cybercrimes cause significant economic damages. For 2015, cyber-attacks resulted in a total average cost of $15 million. While the threats continue to grow, many in the private sector are increasingly taking steps to protect their information systems and the personal information of Americans that they gather in their routine business practices.

To reduce our risk and improve the security of cyberspace, it will take the combined effort of the Federal government, the private sector, our researchers and engineers, and the general public. Although cyber-attacks are becoming more sophisticated, often cyber-attacks are successful because of human error, such as unknowingly opening a malicious email or allowing one's credentials to be compromised. Part of our effort must be to educate the public. Another part must be to better understand human behavior in order to make new tools and technologies more effective, such as the work being done at NIST and elsewhere to move beyond passwords.

I look forward to hearing from our witnesses today about industry cybersecurity best practices as well as opportunities for public-private partnerships that could help address our shared cybersecurity challenges. I'm also interested in hearing to what extent private businesses and organizations voluntarily implement FISMA standards developed by NIST, and how you may be participating in or benefiting from other efforts at NIST, including the Cybersecurity Center for Excellence and the Framework for Critical Infrastructure.

Thank you and I yield back the balance of my time.