OPENING STATEMENT

Rep. Daniel Lipinski (D-IL)
Subcommittee on Research & Technology
Committee on Science, Space, and Technology

The Expanding Cyber Threat

February 27, 2015

Thank you, Chairwoman Comstock for holding this hearing on cybersecurity, and welcome to the Science, Space, and Technology Committee. I look forward to working with you this Congress. I also want to thank our witnesses for being here today.

Cybersecurity remains a timely topic, it is a topic on which this Committee has an important role, and finally it is one for which we have much more agreement than disagreement across the aisle. So I am pleased that the Research and Technology Subcommittee is starting off the new Congress with this hearing.

Cybercrimes are ever-increasing. The threats are not only growing in number, but in the level of sophistication. Some cases, such as the recent Sony hack and the 2013 Target breach, are very high profile and are covered extensively in the media. Many, many more receive less attention. Two weeks ago, the *New York Times* reported that hacking has gone mainstream. A website has been created to connect hackers to potential clients, and as of early January, at least 500 hacking jobs had been laid out to bid and at least 50 hackers signed up to do the dirty work.

Cybercrime threatens our privacy, our pocketbooks, our safety, our economy, and our national security. Arriving at any precise value of losses to the American people and the American economy is impossible. But the Center for Strategic and International Studies, in a study completed last June, reported that, on average, the U.S. loses 0.64 percent of its GDP to cybercrime. I know we will hear more from our witnesses about the extent and nature of the cyber threat.

Two years ago, President Obama signed an Executive Order to begin the process of strengthening our networks and critical infrastructure against cyberattack by increasing information sharing and establishing a framework for the development of standards and best practices. NIST plays a key role in several of these efforts, and we will hear about some of it today. But the President reminded us just two weeks ago that Congress must still act to pass comprehensive cybersecurity legislation.

Fortunately, this is one area in which this Committee has responsibly legislated in the last few years. At the very end of 2014, the Cybersecurity Enhancement Act that I joined Mr. McCaul in introducing for several Congresses in a row was finally signed into law. That law does a number of things.

- It strengthens coordination and strategic planning for federal cybersecurity R&D;
- It codifies the NIST-led voluntary Framework in the President's Executive Order;
- It strengthens and streamlines the NIST-led processes by which federal agencies track security risks to their own systems;
- It codifies NSF's longstanding cybersecurity scholarship for service program to ensure more qualified cyber experts are employed by federal, state, and local governments;
- It codifies the cybersecurity education and awareness efforts led by NIST;
- And finally it authorizes several more important actions and programs led by NIST.

I list all of these things in part so that all of the new Members to the Science Committee understand just how central NIST is to our government's cybersecurity efforts. It is one of the most important least-known agencies in our government. I look forward to hearing about NIST's efforts from Dr. Romine, and how the new law will further strengthen NIST's leadership role in cybersecurity. I also look forward to hearing from Dr. Kurose about the critical and potentially transformative cybersecurity research programs funded by the National Science Foundation. And I look forward to hearing from the other three witnesses who can help educate us further about the importance of public-private partnerships and the areas where this Committee might look to address cybersecurity vulnerabilities during this Congress.

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