Committee on Science, Space, and Technology
Subcommittee on Technology
Cyber R&D Challenges and Solutions
February 26, 2013

Opening Statement
By
Ranking Member Frederica Wilson

Thank you, Chairman Massie for holding this joint hearing on cybersecurity, and thank you to our witnesses for being here today. Before I begin, I'd like to say that I am pleased to be the new Ranking Member of the Technology Subcommittee. As a longtime educator, I am a big believer in the power of scientific innovation. Mr. Chairman, I am looking forward to working with you this Congress to help enable innovation that creates jobs and makes our nation more secure.

Today's hearing is a perfect example of the work this Subcommittee can do to bolster national security. Cyber crimes are ever-increasing. In fact, the number of attacks reported by federal agencies increased by 782 percent between 2006 and 2012.
The threats to federal systems and our critical infrastructure are not only growing in number, but in the level of sophistication.

Over the last month alone, The New York Times, The Wall Street Journal, The Washington Post, Twitter, and Facebook have all confirmed that they have been the target of sophisticated cyber attacks. These crimes may include identity theft, intellectual property theft, service disruptions, and even espionage.

We're beginning to suffer the costs of cybercrime. A recent study found that cybercrime now costs a U.S. business $8.9 million on average per year. The problem is so pervasive that security experts now joke that there are only two types of American companies these days: *those that have been hacked and those that don't know they've been hacked.*

Earlier this month, the President signed an executive order that begins the process of strengthening our networks and critical infrastructure against cyber attack by increasing information sharing and establishing a framework for the development of standards and best practices. But the President also acknowledged that Congress must act to pass comprehensive cybersecurity legislation.

The bipartisan legislation introduced by our colleagues Mr. McCaul and Mr. Lipiniski, and under consideration today, should be part of this comprehensive package. I am looking forward to hearing any recommendations our witnesses might have about how to improve the legislation. Additionally, I hope to hear more from our witnesses about their thoughts on the role the executive order outlines for NIST. In the past, Congress has asked NIST to bring the private sector together to accelerate the development of voluntary standards.
It seems appropriate that NIST be tasked with a similar role in cybersecurity—especially in light of their expertise in this field.

Finally, I'd be remiss if I did not mention the potential impact sequestration will have on our ability to deter, defend, and recover from cyber attacks. In a letter to appropriators, the National Science Foundation indicated that "vital investments in research and development would be jeopardized" and that one of the areas that could be impacted by sequestration is research into advances in cybersecurity.

The Department of Homeland Security's Science and Technology Directorate plays a large role in the development and deployment of cybersecurity technologies. The Directorate has indicated that under sequestration they will have to cut their cybersecurity research by 30 percent, eliminating research in data privacy, identity management, cybersecurity forensics, and security for cloud based systems.

The need to invest in research and development is critical as cyber threats continue to grow and evolve. I hope we will not let sequestration delay and derail these essential investments.