Opening Statement of Chairman Thomas R. Carper
Strengthening Public-Private Partnerships to Reduce Cyber Risk to our Nation's Critical Infrastructure
March 26, 2014

As prepared for delivery:

A little more than a year ago, President Obama signed an Executive Order which put into place a number of efforts intended to enhance our nation's cybersecurity. We are here today to see what kind of progress has been made in implementing the Order and to gather other ideas about better securing our critical infrastructure from cyber attacks.

Every day, sophisticated criminals, hackers, and even nation states are probing our government agencies, universities, major retailers and critical infrastructure.

They are looking for weak spots in our defenses. They want to exploit these weaknesses to cause disruptions, steal our personal information and trade secrets, or even worse, cause us physical harm.

While we have been able to hold off some of these cyber attacks, anyone who has examined this issue even casually will tell you that our adversaries are getting into our systems every day. Earlier this week, for instance, the Washington Post reported that Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked.

Still, we have made some significant progress over the last year. For example, DHS and other federal agencies have taken steps to share more timely and actionable cyber threat information with the private sector.

And I know in talking to many businesses that the cooperation between the federal government and industry on dealing with the cyber threat has gotten much better.

One of the most significant accomplishments over the last year though, was the release of a voluntary cybersecurity framework. This framework provides those who choose to implement it – whether they be government entities, utilities, or businesses large and small - with a common-but-flexible set of best practices and standards they can use to better secure their systems. I tend to think of the framework as a "blueprint" or "roadmap" for stronger cybersecurity.

The President's Executive Order called on the National Institute of Standards Technology, including Ms. Dodson here, to work hand-in-hand with industry to develop the framework. It is a living document, so NIST, working with industry, will continue to update the framework to include lessons learned and address the latest cyber threats.

From what I understand, the development of the framework ran very smoothly and the end result is a product that has been well-received by many stakeholders.

In fact, just last week in Delaware, I sat down with a group of cybersecurity experts at DuPont who were all extremely appreciative of the public-private collaboration that went into developing the framework. To NIST and all the partners that worked on this framework together, I say 'Bravo Zulu.' But, I think we can all agree that we have not yet crossed the finish line.

Right now, many organizations across the nation are actively analyzing the framework to determine how they can use it and incorporate it into their own cyber practices. I commend those efforts, and I am pleased that we have several witnesses with us today who will share their thoughts on using the framework.

Naturally, not every company or state is ready to use the framework. Some may not even really understand what it is. To these organizations, I say, help is around the corner.

"Under the leadership of the very talented Dr. Phyllis Schneck, the Department of Homeland Security has launched a new voluntary program to assist organizations in adopting the framework.

This program will be incredibly important to the success of the framework. And we will be closely monitoring its progress to ensure it is providing the right tools and information to stakeholders. For instance, we need to make sure our nation's small and medium-sized businesses are getting the attention they need to really drill down on the framework.

At the end of the day, I think the question that we are all asking is whether or not the framework will help improve our nation's cybersecurity. While it might be too early to answer this key question, I do believe that the framework itself provides a much a much needed roadmap for companies that want to improve their cybersecurity. This is a great first step.

Of course, the framework will only be successful if companies actually use it – so it is time for industry to roll up their sleeves and put this roadmap to use. It makes business sense too. In the words of Dr. Pat Gallagher, the head of NIST and now Acting Deputy Secretary of Commerce, "good cyber security is good business."

When you consider the threat we are up against, however, I think we can all agree that there is much more that needs to be done. That is why I continue to believe that bipartisan legislation is the best long-term solution to address this growing threat. I have been working hard with my Ranking Member, Dr. Coburn, in an attempt to produce such legislation.

For example, I believe we need to modernize the way we protect our federal networks from cyber attacks.

We also need to clarify and strengthen the public-private partnership we want Department of Homeland Security and industry to have regarding cybersecurity.

We need to make information sharing easier so that companies can freely share best practices and threat information with each other, and with the federal government. Finally, we need continue to develop the next generation of cyber professionals and enhance our cyber research and development efforts right here at home.

Last week, I had the privilege of visiting a new cybersecurity class at the University of Delaware. I was incredibly impressed with the students and was even told that the class was "oversubscribed." That is a good problem to have.

Those students at the University of Delaware, they get it. They understand what cybersecurity means and how important it is for our economic and national security. Our friends with us today, they understand it too.

But for some other folks, this is just a hard issue to grasp.

It is my hope that the framework can jumpstart a new conversation about cybersecurity in our country. And it is my hope that we can come together as a nation – government and industry, Democrat and Republican – and work together to tackle this growing threat we face.

###