Opening Statement of Ranking Member Thomas R. Carper:
"Protecting America from Cyber Attacks: The Importance of Information Sharing"
January 28, 2015

As prepared for delivery:

I would like to thank the Chairman for calling this very important and timely hearing. I believe it is very fitting that our first hearing this Congress will focus on cybersecurity. This is an area where our Committee achieved a number of key legislative successes last year to strengthen our nation's defenses against cyberattacks. We need to make further strengthening those defenses a top priority again this year.

Over the last few years, we have witnessed many troubling cyber attacks. We've seen banks get hit by huge denial-of-service attacks intended to frustrate customers and make it harder to do business. We've seen retailers big and small suffer massive data breaches that have put Americans' finances at risk. And we've seen government agencies fall victim to cyber intrusions time and time again, threatening our national security.

What we saw happen to Sony Pictures at the end of last year, however, was in many respects a turning point. Some have called it 'a game changer' when it comes to spreading awareness of the threats we face. Instead of just having data stolen, Sony Pictures was the victim of a destructive cyber attack at the hands of another nation – North Korea. The attack destroyed thousands of computers and caused data on its systems to simply vanish. We have heard about these types of destructive attacks in other countries, but never one of this magnitude here on U.S. soil. This devastating attack did not stop in cyberspace. It was coupled with threats of violence against American moviegoers and an assault on the values we cherish.

Many experts believe that destructive cyber attacks will grow even more common. In fact, just two months ago, the Director of the National Security Agency, Admiral Mike Rogers, stated that we will likely see a dramatic cyber attack on America in the next decade. He also said that other countries have the capabilities today to disrupt our critical infrastructure.

Last Congress, our Committee took several important steps to better secure our country against this ever-growing threat, sending a number of bipartisan cybersecurity bills to the President's desk for his signature. We passed a bill codifying the basic functions of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security. This is the information sharing hub where the federal government interacts with critical infrastructure companies on cybersecurity. This new law provides our private sector partners in cybersecurity greater certainty that they have someone to work with in combatting the threats they face every day. It also encourages greater sharing of cyber threat information.

We also enacted legislation to modernize how Federal agencies secure their networks, scrapping an extensive and dated paperwork-heavy system with a more nimble one based on the latest and most-effective strategies. The new law also requires agencies to share more cyber threat information with each other. And finally, we passed two laws to help the Department of Homeland Security hire and retain the top-level talent it needs to fulfill its cyber missions.

While we made important progress last year, there are still important pieces of cyber legislation on our 'to do' list. Today, we will be focusing on one of these issues – cyber threat information sharing.

While businesses and the government appear to be getting better at sharing information all the time, more must be done to take the remaining uncertainty and guess work out of the process. This is necessary because the lines of communication between businesses and government are unfortunately not always clear. Often times, legal ambiguities make companies think twice about sharing cyber threat information with the government or their peers. In some cases, companies are uncertain about what they can do to defend their own networks. Legislation can fix these problems.

I have a very strong interest in introducing and moving strong, sensible legislation to better enable the sharing of cyber threat information. And, I expect that this Committee – with its jurisdiction over the Department of Homeland Security – will be very engaged in cyber threat information sharing legislation this Congress. That said, I recognize that we share the responsibility of figuring out the right solution for information sharing with many stakeholders, including the Executive Branch and other Senate committees.

In fact, our friends on the Intelligence Committee, particularly Senators Diane Feinstein and our former colleague Saxby Chambliss, worked tirelessly to move an information sharing bill last Congress. Senator Feinstein also had an information sharing bill in the Congress before that. And of course, this Administration has made cyber threat information sharing a priority.

I was pleased to see the President put forward his own legislative proposal to improve information sharing. While not perfect, I believe it includes constructive proposals that will help us continue the conversation on this issue. I look forward to hearing from our panel today about the President's proposal as Senator Johnson and I and our colleagues consider our options for moving legislation. We must find a legislative solution that will address our information sharing needs while upholding the civil liberties we all cherish. And we must move with a sense of urgency on this important legislation.

I should hasten to add that an information-sharing bill, however, is not a silver bullet. We need to pursue additional ways to help businesses better protect their networks and deter our would-be attackers. A national data security and breach notification standard, then, is also an essential tool that I intend to pursue this Congress.

On Election Day, American voters sent Congress a clear message: they want us to work together in a bipartisan fashion, they want us to achieve real results, and they want us to take actions that help grow our economy. Passing bipartisan information security and data breach measures would do all three of those things.

In closing, I think it's important to note that in approximately one month, the current funding for the Department of Homeland Security will expire. We cannot let this happen. The threats to our country in cyberspace and in any number of areas are just too great, and we will discuss some of those today. DHS has a lot to say grace over, and we do them no favors by playing games with their budget. We need to promptly pass a clean bill to fund DHS for the rest of this fiscal year so

that department and its employees can continue to effectively carry out their critical role of helping to keep Americans safe in an ever more dangerous world.