Statement of Ranking Member Tom Carper
"Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions"

Wednesday, May 18, 2016

As prepared for delivery:

Thank you, Mr. Chairman. Today, we are discussing a subject of immense importance to America – the security of our critical infrastructure. And when we talk about critical infrastructure, we're talking about the things we rely on every day: our supply of electricity, our drinking water, and even the financial system that supports our economy. Unfortunately, our electricity and water utilities, as well as our banks, are at risk every day in a number of ways. We've heard a lot lately about criminals and terrorists targeting them online, but these critical services are also at risk due to any number of other hazards such as violent storms, earthquakes, and even failure due to aging and under-investment.

Fortunately Congress, the Administration, and the private sector have been hard at work to address vulnerabilities in a number of these areas. We have passed several bills in recent years to help make our critical infrastructure more secure and resilient. In 2014, members of this committee worked for many months to enact legislation to reauthorize and enhance the Chemical Facilities Anti-Terrorism Standards (CFATS) program at the Department of Homeland Security. This program is our frontline defense against terrorist attacks against companies that store, manufacture, and process hazardous chemicals. Also in 2014, the President signed a bill to enhance the cybersecurity center at DHS that works with critical infrastructure owners to prevent and respond to cyber attacks. That same year we also gave DHS the authority to hire the best and brightest cyber talent. And just last year, the President signed the Cybersecurity Act of 2015, which our committee played a key role in drafting. This crucial new law makes collaboration between the federal government and companies grappling with cyber-attacks easier and faster.

This year, we are working hard to ensure proper implementation of these laws. We are also working to streamline and strengthen the office within DHS that helps protect critical infrastructure. That office is currently called the National Protection and Programs Directorate, or NPPD. This name is quite a mouthful and really doesn't tell the American people much about what the men and women who do there to better secure our critical infrastructure. As the Chairman knows, my staff and I have been working with DHS on legislation to streamline this office so that it can be a better partner with industry. We do this in part by elevating its cyber functions and making sure that physical and cyber threats to our critical infrastructure are assessed jointly, so the 'left hand' knows what the 'right hand' is doing.

We also want to rename the Directorate as the Agency for Cyber and Infrastructure Security. Doing so will make it clearer that, when there's a problem with a vulnerability in the electric grid or some other piece of critical infrastructure, there's no question about who in the federal government can help – and who can be held accountable when things go wrong and singled out for praise when things go right. And as we know, unfortunately, bad things oftentimes do happen. The important thing is to be prepared for when they do. So I credit the men and women of DHS, including in NPPD and elsewhere, for the hard work they do to ensure our critical

infrastructure is secure and resilient. As one example of this important work, DHS conducts on-site assessments and incident response for dozens of critical infrastructure companies every year.

When we talk about critical infrastructure – especially systems that we cannot afford to lose even for a few minutes – this means building resiliency into our policies and practices. Today's discussion about critical infrastructure reminds me of one very promising technology that is already helping to make our country more resilient to electric grid outages. A company called Bloom Energy manufactures fuel cells in Newark, Delaware. These stationary fuel cells do not require additional transmission capability to move electricity to the end user, meaning reliable electricity can be provided even when the electric grid goes down. Innovative solutions like these can help us be more prepared for a wide variety of threats.

With that, I would like to thank our witnesses for being here today and helping us learn more about critical infrastructure security. I look forward to learning more about what we can be doing better in this space.