

**Opening Statement of Chairman Thomas R. Carper:
“Cybersecurity, Terrorism, and Beyond:
Addressing Evolving Threats to the Homeland”
September 10, 2014**

As prepared for delivery:

Almost every year, this committee holds a hearing to review a multitude of threats to our homeland and examine how our government is working to counter them. We routinely hear from the Department of Homeland Security, the FBI and the National Counter Terrorism Center about how we can best keep Americans safe from those who seek to carry out deadly attacks against our country and its people. We also hear about actors in cyberspace that want to drain our bank accounts, shut down our financial system and our electric grid, steal our individually identifiable information and our identities, as well as the R & D that will enable American businesses and our military to remain pre-eminent in the world.

Assessing these ever-changing, broad threats and making sure our government continues to hone its ability to stop them remains a top priority for this committee, particularly as we approach another 9/11 anniversary. This year, our hearing takes on an added significance, as our nation confronts a growing terrorist threat in Iraq and Syria. As we sit here today, our military is engaging in limited airstrikes in Iraq in an effort to dislodge and repel that threat. Later this evening, President Obama will address our nation. He is expected to share with us and the world the steps that he is recommending be taken in Iraq and in Syria to reverse the expansion of the Islamic State of Iraq and Syria and enable the people who live in those countries to reclaim their lives.

Much of the world has been exposed to a steady stream of deeply disturbing images from that region in recent weeks. Brutal executions. Human rights atrocities. Repression of women. And a seemingly endless procession of masked militants defiantly waiving the black flag of jihad in celebration of their brutality. Effectively addressing the threat from the newly-proclaimed Islamic State of Iraq and Syria will require a multifaceted strategy. That strategy will need a military component and the development of a robust international coalition to execute it. Among the goals of that strategy is to ensure that the Islamic State of Iraq and Syria does not establish a long-term safe haven from which it can launch attacks against either our allies or our homeland – much like we saw with al Qaeda in the days before 9/11.

Today, we will examine the steps that our federal government has already taken, along with the steps we still need to take, to prevent this from happening. We will drill down on this threat and its impact on our homeland, both in this open hearing as well as in a classified briefing directly following. That's not all we're going to do, though. In addition to examining the more conventional terrorist threat the instability in Iraq and Syria may pose, we will also closely examine another major threat that affects our homeland daily: cyber attacks.

Every day, nation states and their affiliates, criminals, terrorists, and hackers launch cyber attacks against our government agencies, our businesses, and important parts of our daily lives such utilities and financial networks. Some of these actors want to steal our sensitive information to sell it on the black market or to gain a competitive edge. Others are trying to make a political point. Some, however, would like to use a cyber attack to cause wide-scale economic damage or even physical harm. Many of them are good at it, and they're getting even better. We need to stay a step ahead of them. Today, we'll hear in the open portion of this hearing and also in the closed portion how we plan to do that, not unlike the steps we've taken to address terror threats in the wake of 9/11.

Congress clearly has a role to play here. Actually, several roles. One of them is an oversight role. It's one that we take very seriously. Another is a legislative role that involves developing legislation to help enable America to anticipate and repel the cyber attacks that we face on an almost 24/7 basis today. In the last several months, this Committee has completed action and reported three separate cyber bills unanimously to the full Senate. One bill would significantly enhance the capabilities of the Department of Homeland Security's cyber workforce. Another would better protect federal agencies from cyber attack. And, a third would codify the cyber center that the Department uses to monitor and respond to attacks to strengthen its ability to do so.

Yesterday, in an op-ed in "The Hill" newspaper, Secretary Johnson recognized the bipartisan efforts of this Committee and talked about the critical need to pass cyber legislation this Congress – I couldn't agree more. In closing, as we mark the anniversary of 9/11 tomorrow, we must keep in mind one of the key lessons we learned since that fateful day thirteen years ago—the threat is always evolving. Not that long ago, crooks used to have to rob a bank to steal our money. Now, they can click a button on a distant computer and accomplish the same goal. Nation states and rival businesses used to employ corporate insiders or retirees to steal company secrets. Now, they send a spear-phishing email. And terrorists used to be a distant threat in the mountains of Afghanistan or Pakistan. Now, an increasing number of them are homegrown. They may be using European, or even, American passports.

So as the threats become more sophisticated, more elusive, and more diffuse, we need to remain ever vigilant to ensure that our government is nimble enough to keep up with tomorrow's threats as they confront us. We have come a long way since 9/11. In many respects, we are more secure than we were on this day thirteen years ago, but the world in which we live remains a dangerous place, so there is always more work to do. When it comes to securing the homeland and anticipating the next threat, we owe it to the American people to strive for perfection. The consequences of failure are simply too high, and the costs too severe.

I'm pleased that we have with us today a panel of witnesses who work together every day to tackle the terrorist and cyber threats we face. Let me express my gratitude to each of you for your testimony and also thank you for your service to our country.

###