Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Markup of H.R. 3696 - the "National Cybersecurity and Critical Infrastructure Protection Act of 2013"

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
January 15, 2014

Mr. Chairman, I am very pleased that we are considering H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2013." This bipartisan measure is, in many ways, the culmination of years of oversight work by this Committee. It not only sends a strong message of support for the Department of Homeland Security as the lead civilian agency for cybersecurity but also pays special attention to the challenge of bolstering the cybersecurity of critical infrastructure.

In recent years, we have come to understand that cybersecurity has to be woven into everything that a company, government, or an individual does, from running the most intricate machinery to everyday participation in social media.

America used to depend on the two oceans to protect us from invasion. Interconnectedness, resulting from advancements in technology, has fostered great economic, scientific, social, and cultural rewards. At the same time, that same interconnectedness allows our enemies to do harm without ever stepping foot on U.S. soil.

One of the strengths of H.R. 3696 is that it emphasizes voluntary information sharing and collaboration between the Department and critical infrastructure owners and operators to address this national threat. Importantly, it does so in a manner that is consistent with our constitutional values and principles.

The fact that the American Civil Liberties Union called the bill "pro-security and pro-privacy" underscores that H.R. 3696, as introduced, effectively avoids the privacy and civil liberties pitfalls that plagued other cyber legislation.

Simply put, as introduced, H.R. 3696, does not create broad exceptions to the privacy laws for cybersecurity but, instead, leverages existing private-public partnerships such as Information Sharing and Analysis Centers and Sector Coordinating Councils.

For DHS to be effective in its cybersecurity mission, it must have a workforce in place to meet this challenge. A long-standing interest of mine has been how best to help DHS meet its cyber workforce needs. To that end, I authored legislation that the Committee unanimously approved in October to help ensure that DHS has the "boots-on-the-ground" it needs to meet its diverse cybersecurity mission. I thank you, Chairman Meehan, for the support you have shown for my efforts and the spirit of collaboration that you have shown.

Today's mark-up represents an important moment for the Committee and the 113th Congress. At the beginning of the Congress, expectations were high for some legislative action in the area of cybersecurity. It has taken some time to get here but what we have before us is something solid that sets forth what DHS, as the lead civilian agency for cybersecurity, must do.

We have seen cybersecurity legislation fail to become law multiple times. While President Obama's Executive Order is making progress in attempts to shore up some cyber weaknesses, more work needs to be done. With this cybersecurity legislation, we will be doing our part, as DHS' authorizers, to raise the level of cybersecurity, particularly within the Federal government and critical infrastructure.