Opening Statement - Ranking Member Cedric L. Richmond (D-LA)

The Current State of DHS Private Sector Engagement for Cybersecurity

Subcommittee on Cybersecurity & Infrastructure Protection

Thursday, March 9, 2017

Cybersecurity issues dominated the 2016 election. From the security of Secretary Clinton's server, to Vladimir Putin ordering cyber attacks on U.S. election systems, to WikiLeaks publishing the private emails of prominent Democratic figures – America got a crash-course in cybersecurity.

Before he was sworn in, President Trump said he would direct the Department of Defense and the Joint Chiefs to develop "a comprehensive plan to protect America's vital infrastructure from cyberattacks, and all other form of attacks" on his first day in office.

While I share the President's desire to better protect critical infrastructure, directing the Pentagon to take on cybersecurity in the private sector would represent a radical departure from how the government manages cybersecurity.

Since 2001, DHS has been the lead agency responsible for coordinating Federal efforts to protect critical infrastructure and, in that capacity, has made major strides in cyber information sharing among critical infrastructure owners and operators.

Then two years ago, with input from some of the witnesses assembled on this panel, legislation was signed into law codifying DHS' role as the lead civilian interface for information sharing. Since that time, DHS has ramped up its efforts to partner with critical infrastructure.

We often say on this Committee that the threat landscape is constantly evolving. When it comes to cybersecurity, the volume, complexity and scale of attacks grow exponentially with each passing day. To meet this challenge, the culture around cyber information sharing needs to shift – *just* as it needed to shift after 9/11, when Federal law enforcement and intelligence agencies moved from a "need to know" to "need to share" culture.

As we work to enhance the quality of information sharing, we must not lose sight of the obligations of all involved to protect the personal information of Americans on impacted networks. I am glad that Ms. Green is here to talk with us about these obligations. I also look forward to talking with *all* the witnesses about what, from their perspectives, DHS (and specifically the NCCIC) could be doing better.

Last year, Congress enacted legislation I authored to make sure DHS is carrying out its diverse portfolio of cybersecurity responsibilities in a strategic manner. In a couple of weeks, DHS should be transmitting to Congress it's first-ever Department-wide cybersecurity strategy. When we see the strategy, I may want to engage with you on your thoughts.

Finally, while I recognize that the long-awaited Executive Order on cybersecurity has not yet been issued, it would be good to hear your thoughts on what we've seen so far from President Trump on cybersecurity.