Opening Statement of Ranking Member Cedric Richmond (D-LA)

Subcommittee on Cybersecurity and Infrastructure Protection

Examining DHS's Cybersecurity Mission

Tuesday, October 3, 2017

I am pleased that we are kicking off cybersecurity awareness month by talking to the Department of Homeland Security about its cybersecurity mission and how Congress can help ensure DHS is well-positioned to protect critical infrastructure from cyber attacks.

Before I begin, however, I would like to send my condolences to the families of the victims of Sunday night's horrific shooting in Las Vegas. To the survivors, you are in our thoughts. To the brave first responders who ran into danger when everyone else was running away from it, we are grateful.

The Democrats on this Committee have said this before, but it bears repeating: At some point, the Majority is going to have to stand up to the gun lobby and enact responsible gun control legislation.

And, as the Congressman representing New Orleans, I cannot sit silently as the President insults the hurricane survivors of Puerto Rico and the San Juan Mayor who is trying to help them.

Having seen people grieve the loss of their homes and businesses and struggle to piece their lives back together, I can tell you the last thing the people of Puerto Rico need are insults from the President. I urge the President to take a break from Twitter, roll up his sleeves, and get to work.

Turning to the issue at hand, as I mentioned, I represent New Orleans, which has significant energy sector assets. Last month, we heard disturbing reports of a "new wave" of efforts to breach energy sector networks in the United States. According to Symantec, in some cases, hackers achieved unprecedented access to operational systems.

In light of these reports, I am interested to know how the Department of Homeland Security and the Department of Energy are working together to secure energy sector networks and make them resilient.

Additionally, as a Member of this Committee and of the Congressional Task Force on Election Security, I am eager to hear about DHS' activities to secure our election systems.

Although the Administration's commitment to the critical infrastructure designation appeared to waver earlier this year, I was encouraged when Acting Secretary Duke told Committee Democrats last month that "[t]here are no plans" to rescind the designation.

With that commitment, I look forward to hearing about the progress DHS is making to help State and local governments secure election infrastructure and whether the Department has adequate resources to carry out its responsibilities in that space.

For example, I understand there is a 9-month wait for a Risk and Vulnerability Assessment and that some Secretaries of State have complained about the lengthy clearance process for election officials. I am concerned that these kinds of challenges may deter some states – particularly those hostile to the critical infrastructure designation – from taking full advantage of the resources DHS can bring to bear.

To that point, DHS has struggled to build some of the relationships necessary to executing its election security mission. Although I have heard that DHS is making process in this regard, I am concerned mistakes made notifying certain Secretaries of State that their election infrastructure had been targeted – though it had not been - may have undermined the trust DHS has sought to build.

I will be interested in learning what do you need from Congress to address election infrastructure requests more quickly and build trust within the election infrastructure community.

Finally, when Ms. Manfra testified before the Subcommittee in March, I asked when I could expect the DHS Cybersecurity Strategy. The Strategy, required pursuant to legislation I authored, was due March 23. It still has not been submitted to Congress.

I understand the Trump Administration did not fill leadership positions relevant to the execution of a DHS Cybersecurity Strategy with any real sense of urgency, and ongoing vacancies may be contributing to the delays. But the Strategy is six months overdue, and that is not acceptable.