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

Joint Hearing:

Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security

Wednesday, November 14, 2018

Last night, after years of debate and negotiation, Congress sent H.R. 3359, the *Cybersecurity and Infrastructure Security Agency Act*, to the President's desk. This bipartisan legislation confirms – once again – that Congress intends for DHS to be the primary Federal civilian interface with the private sector on cybersecurity.

I look forward to working with DHS to help the Cybersecurity and Infrastructure Security Agency mature into an operational component and develop the capabilities needed to meet the challenges ahead - from securing election infrastructure to protecting the grid.

The Department of Defense will be an integral partner as DHS carries out its mission to help secure civilian networks. I understand that DOD and DHS recently signed an agreement clarifying how they will coordinate certain cyber activities.

Although I have not seen that agreement, I am hopeful that it will provide clarity for the Departments' roles and responsibilities. I look forward to reviewing the agreement and ask that it be submitted to our Committees as soon as possible.

Moving forward, the success of DOD and DHS' collaboration rests whether the following three things happen:

> (1) DOD and DHS must implement the agreement of understanding at both the policy and operational level;
> (2) DOD and DHS must communicate – and adhere to - their respective roles and responsibilities as they engage with agencies across the Federal government and the private sector; and
> (3) The Administration must request and Congress must provide the funding and resources necessary for DOD and DHS to carry out their missions.

To my first point: too often I hear to testimony from principals about how well their agencies are coordinating only to learn from folks in the field that isn't the case. To me, the problem seems to be that as Federal agencies work to delineate roles and responsibilities on cybersecurity, they reach an agreement on a policy level without involving the operational folks. That invites frustration, confusion, and, at times, mission creep.

Accordingly, I will be interested in learning how DOD and DHS plan to socialize their new agreement on cyber roles and responsibilities throughout their organizations – from policy to operations – and solicit buy-in.

On the second point, it is important that the respective cyber missions of DOD and DHS are communicated and clearly understood throughout the Federal government and among critical infrastructure owners and operators.

Toward that end, I will once again note my strong concern that the White House has eliminated the cybersecurity coordinator. A White House cybersecurity coordinator would be in the best position to ensure the full capabilities from across the Federal government are brought to bear to protect against cyber threats without sowing confusion about who should be doing what.

Finally, we have to provide DOD and DHS the resources it takes to do their jobs. As everyone here will acknowledge, the cyber threats we're facing are evolving. And we have called on DHS to help secure the Federal government, State and local governments, and critical infrastructure from breaches by state and non-state actors. But DOD's cyber funding outpaces DHS' by about 8 to 1. If we expect DHS to be DOD's civilian equivalent for cybersecurity, we need to fund it that way.