Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity and Infrastructure Protection Subcommittee

"The Current State of DHS Private Sector Engagement for Cybersecurity"
March 9, 2017

Remarks as Prepared

Cybersecurity touches every aspect of the world we live in. It's central to every sector of our economy. It's vitally important for the protection of all Americans' most sensitive information, and it's one of the foremost national security challenges of our time.

Our collective ability to combat these threats – with the government and the private sector working together – will be one of the defining public policy challenges of our generation.

Today, the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection meets to hear from key stakeholders on the current state of private sector engagement for DHS' cybersecurity mission. As chairman of this subcommittee, I don't take the responsibility that we as lawmakers in this room have lightly. In a world of rapidly evolving threats, we have been entrusted to be part of the solution, and I believe today's hearing will be an important piece of this ongoing effort.

DHS' cyber mission includes a robust portfolio of existing private sector partnerships – including Information Sharing and Analysis Organizations, the Cyber Information Sharing and Collaboration Program, Sector Coordinating Councils, and the Automated Indicator Sharing Program. Specifically, we hope to learn how these partnerships can be improved and what more DHS can be doing to ensure that these programs and activities are meaningful, substantive and effective.

Today, private sector entities — including U.S. critical infrastructure owners and operators — are on the frontline of the conflict in cyberspace. Our civilian networks face countless attacks every day from bad actors who seek to infiltrate our trusted systems, cripple commerce, and expose Americans' personal information. And every day, these bad actors are using more advanced tactics, techniques and procedures, and higher quality information. It is only through constant and vigilant innovation that their attacks can be prevented, identified and mitigated.

While DHS has made headway in this space and has strengthened many initiatives in its role as the civilian interface and coordinator across the 16 critical infrastructure sectors for cybersecurity, very clearly more work needs to be done. It is not enough to simply have programs "in place." Instead, we must be constantly measuring, bench-marking and setting goals associated with their outcomes. Additionally, DHS needs to become fully operational so it can most effectively carry out the cybersecurity authorities Congress deliberately gave the Department just over a year ago.

Today is the start of a conversation that needs to occur in this new world with this new battlefield. And the start of a new administration provides a clean slate — a perfect opportunity to regroup and reassess before moving forward. An opportunity to ensure that our efforts and resources are aligned with the threat landscape we face.

Several weeks ago in a Homeland Security hearing, I was pleased to have the opportunity to discuss with Secretary Kelly the importance of DHS' cyber mission. What I told him, and what I know the rest of this subcommittee joins me in reinforcing, is that we stand ready to pedal as fast as his agency—and the entire Trump administration demands; because the stakes are too high to do anything less.

In the cyber domain, we are constantly learning new lessons, and it is only by incorporating that knowledge into existing programs and processes that we can continue to move towards greater collaboration and better secured networks. Because while the private sector is on the front lines of our cyber challenges, the federal government, and DHS in particular, has an important role to play as a force multiplier to provide the private sector with every advantage available to defend itself.

In the 115th Congress, this subcommittee will be legislating and conducting rigorous oversight to further strengthen DHS' civilian cyber mission. While the various DHS touchpoints with the private that we will discuss today range in levels of sophistication and size of participant base, they all depend on quality information flowing at a rate that makes it timely and actionable.

Marked changes in the security of our country's cybersecurity posture will only occur in concert with the advancement of the collaborations that we will be discussing today. The combination of information, capacity, and technical expertise needs to be leveraged in partnership at every turn.

We look forward to hearing from the witnesses on these private sector engagement efforts at DHS. Our goal on this topic is to make sure that the private sector has every opportunity and every reason to take full advantage of DHS' cybersecurity programs, so we can continue to work together to secure cyberspace.

Again, thank you to our witnesses for your willingness to share your expertise.

###