HOMELAND SECURITY
COMMITTEE

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

"Maximizing the Value of Cyber Threat Information Sharing"

November 15, 2017

Remarks as Prepared

The severity of the threats we face in cyberspace cannot be overstated. Seemingly every week there's a new headline about a new breach, a new hack, or a new trove of sensitive information that's been compromised. Or there's a new report highlighting the vulnerabilities our government, the private sector, and the American people face from malicious actors.

Those on the operational front of cybersecurity know the threat landscape is evolving at every second. In cyberspace it is nearly impossible to concisely declare who the threat actor is, what they are going to do next and what the cascading effects may be.

The industry method is to prioritize; assess the risks that networks face and prioritize actions to address those risks, and then, keep moving down the list. We in the government must learn from the private sector, assess risks, prioritize mitigation and keep moving.

As I've said before – whether we rise up to our challenges in cyberspace will play a large part in determining whether America remains the world's superpower.

To effectively address these threats, I couldn't agree more with the consensus opinion that the private sector and government need to collaborate. I see a big part of our collective responsibility being to ensure that this collaboration results in, not just rhetoric, but, in a tangible improvement to our country's cybersecurity posture.

What we're here today to examine is perhaps one of the most readily visible and promising forms of this collaboration – the sharing of cyber threat indicators between the private sector and federal government.

In an ecosystem where there is no silver bullet, it's incumbent upon us to conduct rigorous oversight of our information sharing programs to help increase the participation in and volume of cyber threat information shared with the private sector.

The private sector is the frontline for action in cyberspace. In supplying the private sector with an increasing amount of actionable information, we enable our partners to tilt the scales away from our cyber adversaries.

As a Committee, we are continually seeking to learn about possible ways that the Department can help to increase the resilience of private sector networks and fine tune their own efforts for the response, analysis and mitigation of cyber threats. According to DHS, the Automated Indicator Sharing program has shared over 1,335,036 unique indicators, 264,234 shared in September alone, and there are currently 135 non-federal entities participating in AIS, 22 of which are sector specific organizations comprised of groups of companies. DHS estimates the actual reach of AIS indicators to be greater than 10,000 organizations.

As encouraging as it is to see these programs take shape and fill the very important role of convening partners and bridging information sharing from the government to the private sector, we can do better. A recent report from the DHS Office of Inspector General reinforces this notion that there is more work to be done.

Today I look forward to hearing insights and recommendations from our witnesses that we can take back to DHS to continue to strengthen its work sharing cyber threat information. We are tasked with overseeing the crucial DHS programs, knowing that improvements are always possible. Each of you has a unique perspective that will provide invaluable knowledge that we can build on as DHS continues to refine its programs. We will need creative and possibly significant changes to the way that we do things if we expect to gain ground in this fight.

In a space this transformative and this disruptive, the best option is continued partnership. As disparate as the opinion of the private sector and the government can be on many issues, when it comes to security, we are all looking for able, willing and effective partners. The information technology landscape is central to every sector of the economy and every consumer and individual who depend on these systems.

The automation of cyber threat information and the incorporation of classified and unclassified information are areas the government can work on in order to increase the effectiveness of the information being provided to the private sector. It is for that reason that we have gathered this panel of experts to talk to the efficacy of cyber threat information sharing and improvements that can be made.

We look forward to hearing from the witnesses their perspective and understanding of the current state of cyber threat information sharing and their vision and recommendations for a safer future. Again, thank you to our witnesses for your willingness to share your expertise.

###