FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)

Maximizing the Value of Cyber Threat Information Sharing

Subcommittee on Cybersecurity & Infrastructure Protection

November 15, 2017

When this Committee was formed, the nation was still reeling from the September 11, 2001, attacks, and the difficult reality that there were significant information sharing gaps between our intelligence services and law enforcement.

In the months the followed 9/11, the Bush White House warned of "invisible enemies that can strike with a wide variety of weapons" and urged the Congress to stand up a consolidated Department of Homeland Security to protect against the known threats of the day and the unknown threats of the future.

Fifteen years later, the threat landscape has changed dramatically. The "invisible enemies" we face are hackers hiding in plain sight, casing our networks to figure out how to penetrate deeper, steal data, and manipulate networked systems. Fortunately, we do not need to relearn the lessons that 9/11 taught us.

We know that information sharing – in this case, among the public and private sector – can help mitigate or even prevent cyber intrusions. And the Cybersecurity Act of 2015 put in place the mechanisms necessary to facilitate and incentivize robust information sharing. That said, the more things change, the more they stay the same.

After 9/11, we had to overcome an initial reluctance among the intelligence community and law enforcement to liberally share threat information with other agencies that needed to know.

Among other things, information sharing struggled to overcome challenges related to turf wars, fear of reputational damage, and balancing the need to protect information and the need to share it so law enforcement would be able to act.

Similarly, today DHS is struggling to incentivize private sector participation in its cyber threat information sharing platforms, despite Congress acquiescing to demands for strong liability protections.

We hear from stakeholders that the information shared is not actionable, that too much of the information necessary to make indicators actionable is classified, and that there is a lack of confidence in the validity of some indicators because of a lack of adequate vetting.

These are all issues that Federal, State, and local law enforcement had to overcome in the years following 9/11, and, with the help of Congress and DHS, they have made

tremendous progress.

I have every confidence that the same will be true for cyber threat information sharing.

That said, I am concerned that we continue to hear the same pattern of criticisms over DHS cyber threat information products, and I will be interested to know how DHS solicits and incorporates feedback into its programs, from Automated Indicator Sharing (AIS) to the Cyber Information Sharing and Collaboration Program.

I also look forward to hearing from witnesses how DHS can attract better participation non-Federal network owners and operators, who control 80 percent of our nation's networks.

I have heard some concerns that potential participants are holding out until DHS' programs prove greater value, but I would caution that DHS' voluntary programs are only as good as the participants make them. If the private sector refuses to participate in two-way information sharing, DHS' are doomed to fail.

# # #

Media contact: Adam Comis at (202) 225-9978