COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021

September 1, 2021

Establishing a mandatory cyber incident reporting framework at CISA has been a priority for the Homeland Security Committee since last Congress. I applaud Chairwoman Clarke for engaging with stakeholders and working so hard to get the language right. I look forward to continuing to work with her as she continues to refine the text. I would also like to thank Ranking Member Katko for his support of this important legislation.

For a decade and a half, I have served as either Chairman or Ranking Member of this Committee. Over the years, there has been an evolution in thinking about how closely the public and private sector need to collaborate to protect our nation's critical infrastructure. I have seen the Federal government struggle to find the right way for critical infrastructure owners and operators to share security information with the government and to zero in on how to turn that information into an actionable security product.

The *Cybersecurity Information Sharing Act of 2015* was the product of extensive negotiations on the part of both government and industry. When the legislation was finally enacted into law, we had high expectations that it would spur timely sharing and enhance our nation's cybersecurity posture. But the 2015 bill did not fully deliver. There was reluctance among many in the private sector to share information with the Department. And, for its part, the Department struggled to turn what data it did get into something the private sector could use to drive down risk. It focused too much on the volume of indicators shared and not enough on the quality of the information.

For six years, this Committee has engaged with the Department and stakeholders to try to correct course, but over time it has become clear that we need a new approach. Last Congress, former Subcommittee Chair Cedric Richmond offered an amendment to the *National Defense Authorization Act* that would establish a mandatory cyber incident reporting framework at the Cybersecurity and Infrastructure Security Agency. It was included in the House-passed package but was stripped during conference negotiations with the Senate.

Since then, a series of high-profile, high-consequences cyber incidents over the past year, have made it clear we need to take urgent action to improve the way the private sector shares information with the government. As Chairwoman Clarke said in her opening statement, the text we are discussing today is the product of months of stakeholder engagement and bipartisan negotiations to fine tune the bill. And we are here today to further refine the legislation to ensure it serves the purposes of the Federal government and will result in security benefits to covered entities. I am committed to getting this framework right and across the finish line this Congress.

# # #

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