COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Sector Down: Ensuring Critical Infrastructure Resilience

June 27, 2024

In the past several years, significant cyber incidents have demonstrated how an impact on one entity can have wider implications across a critical infrastructure sector or for the broader U.S. economy. Whether it was the Colonial Pipeline ransomware attack in 2021, which resulted in gas shortages across the East Coast, or the recent Change Healthcare ransomware attack, which stalled payments to medical providers across the country, cyber attacks are having real world impacts. Preventing these incidents in the first place must be a top priority, but we must also ensure that critical infrastructure is resilient and that we are adequately prepared to respond and recover from cyber incidents.

One way to improve critical infrastructure resilience is the increased use of cyber insurance, which can encourage better cybersecurity practices and help ensure that companies have the resources to respond to and recover from a cyber incident. We know there are major challenges in the cyber insurance market, with providers reluctant to offer coverage when it is difficult to assess risk.

With the extent of cyber-related losses depending on technological changes and geopolitical uncertainties, cyber insurers have to underwrite policies with limited information. In particular, the potential for catastrophic losses across many entities in the event of a major cyber attack or global conflict creates significant risk for insurers.

I am glad to see the Biden administration has taken the lead on evaluating the potential for a Federal backstop, and I look forward to ongoing engagement with our Administration partners and private sector stakeholders on assessing whether one is needed. I look forward to hearing from our witnesses today about how they see the current state of the cyber insurance market and how the Federal government can play a better role in supporting it.

Additionally, ensuring critical infrastructure resilience will require improving operational collaboration between the Federal government and critical infrastructure. CISA's Joint Cyber Defense Collaborative, or JCDC, has significant potential to facilitate the kind of public-private partnerships that will improve resilience and incident response. Passing Ranking Member Swalwell's legislation to authorize and provide structure to the JCDC is critical to ensuring the JCDC can fully realize operational collaboration going forward.

Today's hearing will give the subcommittee an opportunity to hear from stakeholders about how CISA is collaborating with critical infrastructure and how we can ensure that it provides the necessary support to improve resilience.

# # #

Media contact: Adam Comis at 202-225-9978