COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime

March 11, 2025

Every day, we face efforts by adversaries like China and Russia to breach government and critical infrastructure networks. To combat this risk, we need critical infrastructure entities to strategically increase their cyber defenses, and we need government visibility into the threats we are facing.

Experience has demonstrated that a purely voluntary approach to cybersecurity is insufficient for today's threat landscape and that thoughtful regulations can improve security outcomes. With numerous government agencies having regulatory authority over different critical infrastructure sectors, I understand the concerns from the private sector that regulations may be duplicative or inconsistent, resulting in unnecessarily burdensome compliance efforts.

Additionally, regulations risk being box-checking exercises rather than focusing on improved security outcomes. Therefore, efforts to improve cyber regulatory harmonization are important to ensuring regulations strengthen security and do not instead distract critical infrastructure from their security efforts.

The most meaningful step Congress has taken in recent years to address duplicative cybersecurity regulations was the enactment of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022. Sponsored by Congresswoman Yvette Clarke, this legislation seeks to increase visibility into the current cyber threat landscape, by mandating critical infrastructure entities to report substantial cyber incidents to CISA. It also seeks to harmonize cyber incident reporting requirements by establishing CISA as a central reporting hub that can share cyber incident reports with other relevant agencies.

As I emphasized in comments I submitted to CISA, along with Ranking Member Swalwell and Representative Clarke, the proposed rule issued last year is overly broad and needs significant refinement in order to align with Congress's goals for the program. Additionally, I encourage increased engagement with stakeholders so that CISA can fully understand their concerns and can maximize the effectiveness of this new mandatory cyber incident reporting regime.

That being said, a final CIRCIA rule has tremendous potential to improve the government's understanding of the cyber threats we face and to ultimately reduce the compliance burden on companies by harmonizing incident reporting requirements to a new CIRCIA standard.

By statute, CISA is required to issue a final rule by September of this year. It is essential that CISA work expeditiously to issue a final rule so that we can begin to see the benefits of CIRCIA implementation and so that other agencies can begin work to align their incident reporting regimes to CIRCIA's.

Our adversaries are not pausing their efforts to breach our networks, and we cannot afford to pause our efforts to better defend them.

Relatedly, I am deeply concerned by the new Administration's anti-regulatory attitude that risks undermining our security. While there is a need to streamline cybersecurity regulations, arbitrary policies that require eliminating regulations in order to issue any new ones would prevent agencies from responding to the evolving cyber threat landscape.

Instead, agencies must thoughtfully evaluate how to ensure critical infrastructure entities have the defenses in place to protect our networks and must coordinate efforts to create a more harmonized approach. We must avoid a simplistic discussion of more or less regulation and instead prioritize implementing policies that maximize security outcomes without unnecessary burdens.

I appreciate the support for CIRCIA from our witnesses, and I look forward to their testimony today on how to ensure proper implementation and improved regulatory harmonization.

# # #

Media contact