COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

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

March 11, 2025

I'm glad our subcommittee's first hearing of the Congress is focused on a bipartisan priority: identifying opportunities to improve implementation of the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) and the need to harmonize cyber regulations more broadly.

But before I begin, I would like to take a moment to express my condolences to the family, friends, and constituents of Congressman Sylvester Turner, who passed away last week. His passion for cybersecurity was clear during his participation in the first two Full Committee hearings last month, and we will miss the contributions he would have made to the subcommittee.

Turning to the subject of today's hearing, I agree that compliance costs can outweigh the security benefit of regulations when compliance with duplicative regulations cuts into investments in security. We should not be imposing regulations for regulation's sake. Cybersecurity regulations should be designed to achieve outcomes that are proven to reduce risk and improve security and resilience.

Toward that end, I was pleased to support CIRCIA because it addressed a concrete security gap and will improve the government's ability to detect and disrupt malicious cyber campaigns faster. It also put in place a framework to ensure that covered entities would not need to report the same cyber incident multiple times to multiple regulators.

If a hacker gets into a bank or energy company, we want them to focus on eradicating the threat and getting back up and running. Their first step should not be bringing in a team of lawyers and compliance experts. It should be fixing the problem and re-establishing their services.

I share the concerns raised by our panelists today regarding the scope of the Proposed rule that CISA issued last spring. Notably, I was troubled that the proposed rule did not incorporate the feedback that the private sector provided during the RFI process.

Congress put CISA in charge of the cyber incident reporting rule because it has a record of working collaboratively with the private sector, and our intent was that CISA would engage the private sector to develop a workable rule.

Together with Ranking Member Thompson and Congresswoman Clarke, I submitted comments on the proposed rule urging CISA to more carefully scope the entities, incidents, and information that must be reported.

I also called on CISA to establish an ex parte process to facilitate ongoing engagement with the private sector. With the fall 2025 deadline for issuing a final rule looming, I urge CISA to work quickly to re-engage with the private sector and refine the scope of the rule.

The cyber threats we face are evolving too quickly for any unnecessary delay. I would like to thank Chairman Garbarino and Chairman Green for their focus on improving the nation's cybersecurity posture.

Toward that end, there are at least three key pieces of cybersecurity legislation that I urge the Committee to begin its work on as soon as possible.

First, we must authorize the Joint Cyber Defense Collaborative, CISA's operational collaboration hub. Formal authorization of the JCDC will provide much-needed transparency regarding who can be a member of JCDC and the activities JCDC takes on.

Authorization will help restore trust among JCDC participants, focus JCDC on the activities most likely to drive security benefits, and ensure that it is accountable to both stakeholders and Congress for delivering a return on investment. I appreciated Chairman Green's support of the legislation last Congress and hope to work with my colleagues on a bipartisan basis to refine the bill and broaden support for it this Congress.

Relatedly, the Cybersecurity Information Sharing Act of 2015 is set to expire on September 30th. The bill is the foundation of operational collaboration between the government and the private sector and it must be reauthorized.

Finally, the State and Local Cybersecurity Grant program will also expire on September 30th. The grant program has helped state and local governments across the country improve their ability to defend against and become resilient to sophisticated cyber attacks from our adversaries and other cyber criminals. For months, stakeholders have asked me to do everything in my power to reauthorize the program and I hope my Republican colleagues will support this effort.

Once again, I thank my colleagues for their commitment to moving the ball forward on cybersecurity, and I look forward to working with you to do just that.

# # #

Media contact