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)

Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking

May 1, 2024

I would like to thank the Chairman for giving the Subcommittee the opportunity to hear from the private sector on CISA's proposed cyber incident reporting rule – the Agency's most significant undertaking since it was established. But before I begin, I would like to take a moment to acknowledge the passing of Congressman Donald Payne, Jr.

Although Congressman Payne did not sit on this subcommittee, he had an important impact on CISA, the agency we oversee. Because of Congressman Payne's advocacy, CISA has a standing school security mission within the Infrastructure Security Division, which works to make K-12 schools and universities safer and more secure. He will be greatly missed by Members of this Committee, and we send our most sincere condolences to his family and constituents.

Turning to the subject of today's hearing: implementation of *the Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). CIRCIA was borne out of crisis. A series of high-profile cyber incidents in 2020 and 2021 – like the SolarWinds supply chain attack, the Kaseya compromise, and the Colonial Pipeline ransomware attack – revealed unacceptable blind spots in the Federal government's awareness of malicious cyber activity on U.S. networks. The Federal government was forced to rely on voluntary cyber incident reporting, so we never knew the full extent of who was impacted by the SolarWinds attack, and reporting from Colonial Pipeline was initially delayed. Incomplete information frustrates our ability to understand the motives and goals of our adversaries and delays information sharing – limiting our ability to prevent additional attacks.

Congress passed CIRCIA so CISA and its partners could detect and disrupt malicious cyber campaigns sooner and identify the evolving tactics of our adversaries to more strategically reduce risk. CIRCIA's success rests on getting the final rule right. I appreciate CISA's work to engage with the private sector early in the rulemaking process through the Request for Information and for the thorough NPRM published earlier this month.

Moving forward, it is imperative that CISA strongly consider and incorporate feedback from the private sector, particularly as it refines key definitions - including "covered entity" and "covered cyber incident" - and the required components of cyber incident reports. I also urge CISA to apply lessons learned from programs like Automated Indicator Sharing (AIS).

When Congress authorized AIS nearly a decade ago, we hoped it would achieve some of the same goals we have for CIRCIA today. But AIS never achieved its potential, in part, because it focused on quantity over quality and produced too many reports that lacked value. New technology may enable CISA to draw insights from a higher volume of CIRCIA reports more quickly, but I question whether it will be able to adequately overcome complications from the kind of overreporting that is likely to occur given the breadth of current definitions.

Implementation of CIRCIA will be expensive for both the government and private sector, and we must ensure that it yields real security value. Toward that end, I understand many stakeholders, including some of our witnesses, have requested CISA extend the public comment period by 30 days. I understand that CISA plans to grant that extension and am pleased they are doing so. I also share Chairman Garbarino's frustration with duplicative cyber incident reporting requirements – particularly the SEC rule.

Now that the NPRM is public, I hope the Cyber Incident Reporting Council will redouble its efforts to promote harmonization and that my colleagues in Congress will refrain from passing additional redundant reporting requirements.

I commend my colleagues, especially Ms. Clarke, and the witnesses here today for the work they put into getting CIRCIA across the finish line. CIRCIA showed that improving the nation's cybersecurity posture is a bipartisan goal, and one that the private sector was willing to work with us to accomplish.

Moving forward, I hope we can continue to work together to do big things, like passing important legislation that will improve how the Federal government collaborates with its private sectors partners by authorizing the Joint Cyber Defense Collaborative, JCDC.

I would also like to congratulate CISA on the publication of the NPRM – it is an important milestone in an enormous undertaking, and I look forward to working with CISA to clarify reporting requirements and to build out the analytical capacity necessary to derive actionable insights from CIRCIA reporting.

# # #

Media contact: Adam Comis at 202-225-9978