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)

Sector Down: Ensuring Critical Infrastructure Resilience

June 27, 2024

Malicious cyber actors – whether State-sponsored or cyber criminals – are growing more sophisticated, bolder, and more prolific, and it is costing us. According to the FBI's IC3, cybercrime cost Americans $12.5 billion in 2023, a 22 percent increase in losses from 2022. IC3 also reported that 40 percent of ransomware attacks in 2023 targeted critical infrastructure, making cyber attacks not only expensive but potentially disruptive.

Fortunately, the Biden Administration is leading a range of efforts to bring the unique capabilities of government and the private sector together in new ways to confront evolving cyber threats. The Administration is making important progress on the ambitious agenda it set in the National Cybersecurity Strategy and is modernizing the doctrine that defines how we build collective resilience.

Three initiatives are particularly relevant to this hearing: stabilizing the cyber insurance market; maturing operational collaboration; and improving our ability to understand the cascading effects of cyber attacks so we can mitigate the impacts and respond more dynamically.

Cyber insurance policies have long served as a non-regulatory way to incentivize the adoption of cybersecurity controls and blunt the losses of cyber attacks that overcome network defenses. Unfortunately, increases in the frequency, sophistication, and cost of cyber incidents along with the lack of historical data, lack of models to accurately assess risk, and lack of consistency in terminology and policy coverage have created friction in the cyber insurance market. These dynamics have created a perfect storm – demand for cyber insurance has increased, premiums have gone up, and some insurers are reluctant to write new policies.

The Federal government is in a unique position to bring certainty and stability to the market and I am glad the Biden Administration is working to do just that. Notably, the Administration has prioritized identifying ways the Federal government can help address gaps in the cyber insurance market, particularly related to coverage for Catastrophic Cyber incidents.

The Administration is two years into assessing the need for - and potential structures of - a Federal backstop to a catastrophic cyber event. Without government intervention, we run the risk of cyber insurers being overextended when a catastrophic cyber incident occurs, or writing policies that include so many exemptions that no one can make a claim. Neither scenario is good for our economy or national security, and I look forward to supporting ongoing efforts to find a solution.

The Biden Administration has also re-launched the Cyber Insurance and Data Analysis Working Group (CIDAWG) at CISA, which will help insurers better analyze risk by identifying the security controls that are most effective and improving access to data. Enhancing our ability to evaluate risk will help the cyber insurance market at every level, making cyber insurance more attractive and accessible.

Ultimately higher rates of cyber insurance uptake will reduce systemic risk and yield dividends in resilience.

I'm looking forward to our witnesses' perspectives on what more the Federal government could be doing to strengthen the cyber insurance market. Another area where the government is uniquely suited to bring value is operational collaboration. No other entity has the same convening power or intelligence insights that can help the private sector make better sense of the activity they are seeing on their networks.

I was encouraged that National Security Memorandum 22 recommitted the Administration to building operational collaboration capacity. CISA, the National Coordinator for the Security and Resilience of Critical Infrastructure, has been modernizing its approach to operational collaboration for almost three years with the Joint Cyber Defense Collaborative (JCDC). I will be interested in hearing from the witnesses today how operational collaboration bodies like the JCDC can more strategically leverage public and private sector competencies to boost resilience.

Finally, the government has an important role to play in bringing greater clarity to the interdependencies and cascading consequences of cyber attacks. Earlier this year, for example, we were caught flatfooted after the Change Healthcare ransomware attack. It took too long to understand the broader impacts on the healthcare system, and it limited our ability to respond nimbly.

I was encouraged that NSM-22 directed CISA to identify key interdependencies that would be implicated by cyber attacks so we can better manage risk. And I look forward to working with CISA to improve its ability to conduct that type of analysis.

# # #

Media contact: Adam Comis at 202-225-9978