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)

CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective

March 23, 2023

The Cybersecurity and Infrastructure Protection Subcommittee has a strong history of productive collaboration and, as a result, has enacted meaningful legislation to provide cybersecurity grants to State and local governments, enhanced cybersecurity education and training programs, strengthen Federal network security, and improved our ability to understand and address threats to operational technology. In short, this subcommittee's commitment to bipartisanship has increased capacity and reduced risk for both the public and private sectors. I look forward to building on that record with you this Congress, Mr. Chairman.

Since 2019, Congress has nearly doubled CISA's budget and expanded its authorities significantly. When Congress established CISA four-and-a-half years ago, we envisioned the agency as a sophisticated cybersecurity and infrastructure protection organization. Thanks to bipartisan work on this subcommittee, and the full committee, CISA has matured rapidly, and growing more capable of meeting the challenges of our complex and diverse threat environment.

I am impressed by what CISA has been able to accomplish so far and will always work to support the agency as it continues to adapt to the cybersecurity needs of our federal government, critical infrastructure sector, and private enterprises. From election security to "Shields Up" campaign, CISA has demonstrated an ability to dynamically surge resources to counter emerging threats and collaborate strategically with the private sector.

Looking ahead, Director Easterly has set ambitious goals to modernize CISA's Federal network security programs, tactically engage with entities whose resilience matters most to our national security and our economy, and drive adoption of secure-by-design and secure-by-default. I look forward to learning more about how CISA will work with Congress, its partners in the Executive branch, and the private sector to get the buy-in necessary for success. At the same time, CISA is currently in the process of implementing the cyber incident reporting bill, is on the second year of the State and local cyber grants program, and is executing on a range of new authorities. As we speak, CISA is hosting the inaugural planning summit for the Joint Cyber Defense Collaborative (JCDC), which was established in August 2021.

Everyone I have spoken to about JCDC has told me about its importance to ensuring productive collaboration between CISA and the private sector. The JCDC enabled rapid information sharing among government and private sector partners following Russia's invasion of Ukraine and it was critical to addressing the Log4j vulnerability. But JCDC has existed for a year-and-a-half without a charter or concrete criteria for membership– all of which are essential for the JCDC to provide enduring value. Toward that end, in the coming weeks, I plan to introduce legislation to clarify the activities of the JCDC to improve on its successes and increase its impact.

CISA is also in the process of growing its support for operational technology security by continuing implementation of the CyberSentry program and the *Industrial Control Systems Cybersecurity Training Act*, which I introduced and was signed into law last year. I say this to make the point that while CISA pursues the ambitious agenda set by its leadership - some of which will require this Committee to provide new resources and authorities - it must also effectively execute its existing obligations, including to promote the great training and educational services provided by CISA are widely utilized across industries.

Last Congress, two principles drove the subcommittee's work: First, an increase to the Federal government's visibility of malicious cyber activity and second, pushing resources to entities most vulnerable to cyberattack. As we approach our oversight this Congress, we must ensure the laws we've enacted deliver concrete security value, preserve the trust we built with the private sector to advance critical cybersecurity policy, and work with CISA to address gaps in capacity.

My district is home to countless technology companies, so I know the value the private sector adds to the Federal government's cybersecurity efforts. CISA's collaboration with the private sector is essential to both its Federal network and critical infrastructure activities, and I am glad that we are kicking off the Congress by hearing from some of CISA's most active partners. The testimony from our witnesses today will play a key role in our ongoing oversight of CISA moving forward.

# # #

Media contact: Adam Comis at 202-225-9978