COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure

July 22, 2025

The threat landscape facing our nation is clear—critical infrastructure operational technology is a target for our adversaries, and our cyber defenses are not sufficient for current threats. Under the Biden Administration, Congress and the executive branch took important steps to strengthen OT security.

We invested $1 billion in state and local cybersecurity, and we have seen states use that money to better defend vulnerable water utilities and other high-risk sectors. We enacted the Cyber Incident Reporting for Critical Infrastructure Act so that the Federal government would have better visibility into the threats facing our nation.

CISA established the Joint Cyber Defense Collaborative, including a focus on industrial control system security, and improved its partnerships with sector-risk management agencies, hiring sector-specific experts to coordinate with their partner agencies. CISA further developed cyber performance goals to help critical infrastructure better understand how to improve their security. And the Biden Administration initiated a series of sprints to strengthen the security of specific, under-resourced sectors.

Unfortunately, under the Trump Administration, we have seen the executive branch step back from prioritizing cybersecurity. Secretary Noem has overseen the loss of hundreds of cybersecurity experts from CISA, devastating the agency's capacity for responding to cyber threats. The President's Budget Request included a proposed 25% cut to CISA's programs, including eliminating its efforts to train the OT workforce. Secretary Noem eliminated the Critical Infrastructure Partnership Advisory Council, devastating the private sector's ability to collaborate on cybersecurity threats. And CISA has stalled efforts to carry out its statutorily mandated obligations under CIRCIA.

With a Department of Homeland Security focused exclusively on mass deportations, our nation is more at risk to cyber attacks from China, Russia, Iran, and other adversaries. Unfortunately, Republican leadership in Congress has not been much better. Former Chairman Green failed to move forward legislation to reauthorize the Cybersecurity Information Sharing Act of 2015, leaving us just 17 legislative days away from this vital authority expiring. And House Republicans are proposing to cut CISA's budget by $135 million.

I know this subcommittee recognizes the serious cyber threats facing our nation, and I hope that this hearing will build greater awareness in Congress of the threats facing operational technology and the need for sustained investment in improved security.

# # #

Media contact