COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

**FOR IMMEDIATE RELEASE**

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

## *Data Centers, Telecommunications Networks, and Space-Based Systems: Modernizing DHS's SRMA Role for the Communications and IT Sectors*

**April 29, 2026**

In October 2024, we all learned about Salt Typhoon's successful breach of U.S. telecommunication networks. Chinese state-backed hackers had successfully gained access to the sensitive communications of some of the most high-profile individuals in our country and accessed data on a vast number of Americans. Undetected for months or even years, this wide-ranging incident demonstrated the sophistication of PRC hackers and the vulnerabilities in our own critical infrastructure.

At the time, many thought Salt Typhoon would be a wake-up call about the need to prioritize cybersecurity and invest in improving our cyber defenses. The Biden Administration immediately took steps to better understand the incident and strengthen our defenses by launching a Cyber Safety Review Board investigation into the incident, and the FCC proposed cybersecurity requirements for telecommunications providers.

Unfortunately, starting on January 20th of last year, President Trump's vendetta against CISA – coupled with DOGE's slash and burn approach to dismantling the Federal government - have taken priority over our national security. Under President Trump's leadership, CISA has forced out roughly 1,000 employees or almost a third of its staff. The Cyber Safety Review Board has been disbanded, leaving Congress and the public largely in the dark about how Salt Typhoon's telecommunications breach occurred.

Key public-private collaboration forums, like the Critical Infrastructure Partnership Advisory Council, or CIPAC, have been shut down. And a Republican-controlled Congress has repeatedly failed to pass a long-term reauthorization of the Cybersecurity Information Sharing Act of 2015 despite broad bipartisan support for doing so, leaving the private sector in limbo as to whether the law's vital liability protections will remain in place going forward.

Now, as we face new threats, like rapidly advancing frontier AI models and the war with Iran, CISA's capacity to partner with critical infrastructure and fulfill its sector risk management agency responsibilities is significantly diminished. We must work to right this ship before it's too late.

I appreciate the witnesses for being here today to share their perspectives from the private sector on what more is needed from CISA and Congress to better defend the communications and information technology sectors. We all rely on these sectors every day and breaches of communications and IT networks put Americans' privacy and our national security at risk.

We must act quickly to rebuild CISA's capacity to serve as the sector risk management agency that these sectors need, and CISA must re-establish the public-private partnerships that are necessary for the government and critical infrastructure to productively collaborate to secure the homeland. I hope we can have a candid conversation today about the current status of CISA's SRMA work and how CISA can better support critical infrastructure.

For CISA to serve the communications and information technology sectors properly, it will need to have sufficient staffing and resources to respond to the evolving threat landscape. I am glad that CISA is looking to hire over 300 individuals in the near future, but I worry if qualified applicants will be interested in serving at an agency that has seen its morale destroyed by a hostile administration.

Additionally, CISA must develop the capacity and leadership to not just manage day-to-day activities but to carry out meaningful planning and operations that address new threats and technology. That will require restored partnerships with critical infrastructure. I know the witnesses here today have devoted their careers to improving our national security and have long histories of working with CISA and other Federal agencies to better secure our critical infrastructure.

I look forward to their testimony on what more CISA and this subcommittee can do to strengthen the security of the communications and information technology sectors that are so vital to our security.

# # #

Media contact