COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Unconstrained Actors: Assessing Global Cyber Threats to the Homeland

January 22, 2025

I am encouraged by the Chairman's interest in devoting more of the Committee's time to cybersecurity this Congress. That said, I would be remiss if I did not express concern about what we will be able to achieve.

Over six years ago, bipartisan Members of this Committee came together to support legislation authored by then-Chairman McCaul to establish the Cybersecurity and Infrastructure Security Agency (CISA). When he signed the bill into law, President Trump said, "As the cyber battlespace evolves this new agency will ensure that we confront the full range of threats from nation states, cyber criminals, and other malicious actors, of which there are many."

With the apparent support of the President Trump, Members of this Committee worked together to pass legislation – authored by both Democrats and Republicans – to ensure CISA had the resources and authorities it needed to carry out its critical Federal network and critical infrastructure missions.

Unfortunately, driven by false allegations and conspiracy theories, President Trump and many of my Republican colleagues have soured on CISA. Less than a year-and-a-half ago, over 100 of them voted to cut CISA's funding by 25 percent.

Some of the loudest and most influential voices on the other side want to eliminate the CISA entirely, so even relatively minor bills that touch CISA have been difficult to advance.

I am hopeful that the Committee's focus on cybersecurity this Congress will help Members understand what CISA does and does not do, so we can return to our bipartisan work of making the digital ecosystem safer and more secure.

Bearing that in mind, we have to be clear-eyed about the enormous tasks ahead. Cyber attacks from China, Russia, Iran, and cyber criminals are growing bolder and more prolific.

Last year, former FBI Director Christopher Wray warned that Chinese threat actors like Volt Typhoon pose an imminent threat to U.S. critical infrastructure because they are prepositioning to "physically wreak havoc on our critical infrastructure at a time of its choosing."

Preparing critical infrastructure owners and operators to defend and build resilience to PRC-sponsored cyberattacks requires consistent investment in CISA's programs. And that is to say nothing of its work to help the private sector defend against the espionage threats posed by Salt Typhoon and Silk Typhoon or the threats posed by other adversaries.

During the 116th and 117th Congress, this Committee worked on a bipartisan basis to right-size CISA's budget so it would be well-positioned to defend Federal and critical infrastructure networks against these types of urgent threats.

In fact, in 2020, the top Republican on the Committee advocated that CISA should be a $5 billion agency by 2025. So, I was troubled by the DHS Secretary nominee's testimony last week that she wants a "smaller" CISA because it has "gotten far off mission." Although it was not entirely clear what she meant by that comment, Committee Democrats will oppose any effort to short-change CISA's mission or its workforce.

The Biden-Harris Administration left behind a solid foundation for improving the Nation's cybersecurity that the new Administration can build upon.

Its National Cyber Strategy put the country on path to reduce cyber risk systemically, by shifting the responsibility for security away from our constituents and onto the technology manufacturers and by incentivizing adoption and integration of better security practices.

Its Executive Orders on cybersecurity modernized the Federal government's approach to securing its own networks, sought to address supply chain and third-party risk, and harness the security benefits of new technologies.

For its part, CISA launched the successful State and Local Cybersecurity Grant Program, led efforts to improve the security of the technology we use through its Secure By Design program, and began to mature its operational collaboration activities through the Joint Cyber Defense Collaborative.

The new Administration should not reverse course on this hard-earned progress.

Before I close, I would also like to express my concern regarding the dismissal of the non-government members of advisory committees inside the Department, including the Cyber Safety Review Board and the CISA Advisory Committee. The CSRB is in the process of investigating the Salt Typhoon hack of nine major telecommunications companies, and it is a national security imperative that the investigation be completed expeditiously. I am troubled that the President's attempt to stack the CSRB with loyalists may cause its important work on the Salt Typhoon campaign to be delayed.

The American people deserve better.

# # #

Media contact