STATEMENT OF KATHERINE KUEHN

MEMBER, NATIONAL TECHNOLOGY SECURITY COALITION, AND CHIEF INFORMATION SECURITY OFFICER-IN-RESIDENCE

U.S. HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

HEARING ON
IN DEFENSE OF DEFENSIVE MEASURES: REAUTHORIZING CYBERSECURITY INFORMATION SHARING ACTIVITIES THAT UNDERPIN U.S. NATIONAL CYBER DEFENSES

WEDNESDAY, MAY 15, 2025
2:00 PM

310 CANNON HOUSE OFFICE BUILDING

The **National Technology Security Coalition (NTSC)** is a nonprofit, nonpartisan organization that serves as the preeminent advocacy voice for the Chief Information Security Officer (CISO) and senior security technology executives. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

Chairman Garbarino, Ranking Member Swalwell, and members of the Committee, thank you for the opportunity to testify today in support of reauthorizing the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the importance of public-private partnerships in protecting our national security. My name is Katherine Kuehn, and I am a Board member of the National Technology Security Coalition (NTSC), serving as the CISO-in-Residence.

Established in 2016, the NTSC is a nonprofit, nonpartisan organization that advocates for Chief Information Security Officers, Chief Privacy Officers, and senior security technology executives. NTSC's mission is to advance cybersecurity policies that protect critical infrastructure and foster strong collaboration between the public and private sectors to secure our digital landscape. As part of this mission, we have been deeply involved in shaping the national conversation on cybersecurity, including advocacy for the creation of the Cybersecurity Advisory Committee.

The Cybersecurity Information Sharing Act of 2015 has been a cornerstone of our national cybersecurity strategy. Since its inception, this law has fostered collaboration between industry leaders and federal agencies, enabling the identification and mitigation of cybersecurity threats. The legal protections offered by CISA encourage private organizations to share information without fear of legal repercussions, enhancing the nation's ability to respond to cyberattacks. It facilitates the exchange of critical cyber threat information between private sector companies and the federal government. Through CISA 2015, companies can share indicators of cyber threats, such as software vulnerabilities, malware, and malicious IP addresses, without fearing liability or legal repercussions. This collaborative approach has been instrumental in enhancing the federal government's ability to respond to cyberattacks quickly and effectively.

CISA provides incentives for companies to share cybersecurity threat indicators, such as software vulnerabilities and malware, with the Department of Homeland Security (DHS). This collaboration is crucial for preventing data breaches and attacks from cybercriminals and foreign adversaries. This law has been pivotal in addressing some of the most significant cybersecurity threats over the past decade, including high-profile incidents like the SolarWinds breach and the more recent Volt Typhoon and Salt Typhoon campaigns. These attacks underscore the growing sophistication and scale of cyber threats we face today. As noted by Senators Gary Peters and Mike Rounds, allowing CISA 2015 to lapse would "significantly weaken our cybersecurity ecosystem" and undermine the ability to address these sophisticated threats.

Moreover, a lapse would remove essential liability protections and hinder defensive operations across critical sectors. The protections under CISA 2015 have provided legal certainty for companies that might otherwise hesitate to share critical threat data. This "safe harbor" provision has been crucial in fostering a culture of trust and collaboration. Without this legal protection, the flow of vital threat intelligence would slow, hindering both proactive and reactive cyber defense efforts.

Cybersecurity is a team effort—one that requires collaboration between the government and the private sector. Information sharing is essential for national security as cyber threats become increasingly sophisticated. The current global cyber threat environment demands constant information exchange between these sectors to protect the nation's critical infrastructure. CISA 2015 has been instrumental in supporting this collaboration, particularly through initiatives like

the Joint Cyber Defense Collaborative, which unites federal agencies and leading private-sector cybersecurity firms.

Unfortunately, the recent termination of the Critical Infrastructure Partnership Advisory Council, the disbandment of the Cyber Safety Review Board, and the dismissal of members of the Cybersecurity Advisory Committee have undermined public-private cooperation in cybersecurity. These advisory bodies played a crucial role in fostering dialogue and sharing best practices between the government and industry. Their loss has created a gap in collaboration that must be addressed.

The importance of these public-private partnerships is further emphasized by the fact that critical infrastructure sectors—such as energy, finance, and healthcare—are predominantly managed by private companies. These industries rely on timely and accurate information to protect themselves against attacks from nation-state actors and cybercriminals. Information sharing is crucial for defending against complex, state-sponsored cyberattacks, such as those originating from Russia, China, and North Korea.

The NTSC was directly involved in creating the Cybersecurity Advisory Committee, which was introduced in 2019 through bipartisan legislation. In the 116th Congress, Representatives John Katko, Dan Newhouse, Brian Fitzpatrick, and Dan Lipinski introduced H.R. 1975, the Cybersecurity Advisory Committee Act of 2019, a bill aimed at establishing an advisory committee composed of highly skilled cybersecurity professionals responsible for protecting enterprises across all primary business sectors. The advisory committee would serve as a valuable cyber resource, providing unparalleled insight and expertise to the Director of the Cybersecurity and Infrastructure Security Agency and the Secretary of Homeland Security. The NTSC, in collaboration with these members of Congress and this committee, proposed the idea for the advisory committee and played a central role in its establishment.

The advisory committee was established to provide expert guidance on cybersecurity policy and offer actionable recommendations to enhance the nation's defenses. Its work has been invaluable in shaping cybersecurity policy and ensuring the government remains in close contact with industry leaders. Reinstating this advisory body is essential for ensuring that our cybersecurity policies continue to evolve in response to new threats.

Given the urgency of the current cyber threat landscape, Congress must proceed with a clean reauthorization of CISA 2015. While there will be opportunities to adjust the law in the future, now is not the time for complicated negotiations that could delay reauthorization. A clean reauthorization would preserve the practical framework that facilitates public-private collaboration and provides legal protections for information sharing.

In conclusion, the reauthorization of CISA 2015 is crucial for maintaining the nation’s security and strengthening public-private partnerships in cybersecurity. The law has fostered a collaborative environment that enables the real-time sharing of cyber threat intelligence, helping to defend against attacks from sophisticated adversaries.

We urge Congress to prioritize a clean reauthorization of CISA 2015 to ensure the continued effectiveness of these public-private partnerships and the legal protections they provide.

Furthermore, we urge Congress and the Administration to reinstate advisory bodies, such as CIPAC, CSRB, and CSAC, to strengthen public-private cybersecurity collaborations.

Thank you for your attention to this critical issue. I look forward to addressing any questions you may have.