September 19, 2025

The Honorable Rand Paul
Chairman, Senate Homeland Security & Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Andrew Garbarino
Chairman, House Homeland Security Committee
H2-176 Ford House Office Building
Washington, DC 20515

The Honorable Gary Peters
Ranking Member, Senate Homeland Security & Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bennie Thompson
Ranking Member, House Homeland Security Committee
H2-176 Ford House Office Building
Washington, DC 20515

Dear Senator Paul, Senator Peters, Representative Garbarino, and Representative Thompson:

The Cyber Threat Alliance (CTA) strongly supports reauthorization of the Cybersecurity Intelligence Sharing Act of 2015, and we urge Congress not to let this statute lapse.

CTA is a non-profit threat intelligence sharing organization with 36 member companies founded in 2017. We enable cybersecurity providers to share threat intelligence with each other to better protect customers, support the disruption of malicious cyber actors, and raise the level of cybersecurity across the digital ecosystem. We actively work with other information sharing organizations in the US and around the world.

CISA 2015 provides a clear foundation for our threat intelligence sharing activities. Since our incorporation, more than 55 cybersecurity companies have shared intelligence through the Alliance in some fashion, and CISA 2015 has directly enabled this collaboration. Through its sharing, CTA materially contributes to improved cybersecurity for US businesses and citizens. Without CISA in place, the Alliance would become more difficult to sustain and grow.

CTA members regularly share information in multiple ways. In our automated sharing program, members exchange technical cybersecurity indicators, such as malware, domain names, and universal record locators (URLs), along with context such as the country in which the member detected the indicator or the date and time it was first detected. Currently, members share close to 600,000 of these indicators per day through our platform. While we encourage members to share as much relevant information as possible, we have rules prohibiting members from sharing customer identifying information. Cybersecurity companies have no reason to share customer information with competitors, and they have many contractual requirements to avoid such sharing. As a precaution, CTA has procedures for removing such information from our platform if a member inadvertently shares it, but we have never needed to use those procedures in almost nine years of operation.

CTA members also share finished threat intelligence reports with each other under embargo, usually about 24 to 48 hours in advance of broad publication. This lead time allows members to prepare for an upcoming release, from loading indicators associated with the report into end-point protection systems to preparing talking points to respond to customer inquiries. CTA members regularly rate this program as extremely valuable. CTA enables human- to-human sharing through bi-weekly, virtual meetings of member company researchers and analysts, and we publish joint analytic reports that reflect the combined insights of multiple members on various cybersecurity topics.

CTA has also built a collaboration network with other information sharing organizations, such as Information Sharing and Analysis Centers (ISACs). This network meets quarterly to share insights about adversaries and to ensure that we can have a communication channel during a crisis. This network continues to grow as we add both domestic and international partners.

CISA 2015 facilitates all these sharing activities. The definitions of cyber threat indicator and defensive measure mean that we don't have to negotiate definitions in our legal agreements. We strictly comply with anti-trust laws, but that compliance is made significantly easier due to CISA 2015's anti-trust provisions. The liability protections for sharing activities reduce the worries about potential mistakes made in good faith. Thus, a failure to renew the CISA 2015 authorities would negatively affect CTA's operations. A long-term lapse in CISA 2015 authorities would require a thorough legal review, and some activities might have to shut down temporarily or be substantially scaled back. The increase in legal risk might be more than some companies are willing to take, which could negatively affect our membership. Most information sharing organizations would be in a similar position. In short, letting CISA 2015 lapse would materially worsen US cybersecurity.

While incorporating new concepts, such as indicators of behavior, or widening the scope of defensive measures could be helpful, such updates require a thorough review. Congress should take time to weigh the benefits and costs of any proposed changes before enacting them. Given the length of time required for such a process, Congress should first reauthorize the statute to maintain its significant benefits to the digital ecosystem and then consider whether changes are necessary.

CTA and its members would be happy to answer any questions you or your staff have regarding how CISA 2015 enables our day-to-day cybersecurity work and how that work benefits US national security, economic prosperity, and public health and safety.

Sincerely,

J. Michael Daniel
President & CEO