March 21, 2025

Via Electronic Mail

The Honorable John Thune
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable Charles Schumer
Minority Leader
U.S. Senate
Washington, DC 20510

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
Washington, D.C. 201515

Dear Majority Leader Thune, Minority Leader Schumer, Speaker Johnson, and Minority Leader Jeffries:

As the 119th Congress begins, we urge Congress to extend the September 30, 2025 expiration date for the *Cybersecurity Information Sharing Act*. This bipartisan legislation passed in the wake of the 2015 OPM breach and sought to "encourage public and private sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation."[1] This voluntary information sharing framework has been instrumental in strengthening our collective defense against cybersecurity threats that continue to grow in sophistication and severity.

Recent events underscore the imperative of continuing to support both private-public information sharing and collaboration as well as providing the legal clarity that companies currently count on to share cyber threat information with other companies and across sectors. Nation-state hackers have launched numerous attacks on U.S. critical infrastructure[2] including our communications systems—

[1] Consolidated Appropriations Act, Pub. L. No. 114-113, Div. N, Title I—Cybersecurity Information Sharing Act, 129 Stat. 2935 (2015), 6 U.S.C. § 1501; S. REP. NO. 114–32, at 2 (2015).
[2] Dustin Volz et al., *How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons*, WALL ST. J. (Jan. 4, 2025), https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95; Office of the Dir. of Nat. Intelligence, *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021),

signaling they are positioning for bigger, more disruptive attacks. Federal agencies have similarly been targeted—most recently the Treasury Department in the BeyondTrust breach,[3] but also during the SolarWinds incident where nine agencies were compromised.[4]

In the decade since its enactment, the law has meaningfully improved the capacity and speed with which we can respond to large-scale cyber incidents while establishing clear expectations for privacy and confidentiality. This includes building the structures used by private sector cyber defenders to inform government partners of ongoing cyber threats from malicious actors. Equally as important, the law's antitrust exemption and associated protections have also facilitated broader cyber information sharing between private companies. Private sector cyber defenders, including those from critical infrastructure entities regularly targeted by foreign threat actors, depend on threat indicator sharing from other companies to strengthen their defenses and protect their customers' data. A lapse in the legal framework provided in the Act could limit this sharing. These communication channels are essential for enhancing overall awareness of national security threats and quickly responding to incidents. Given that value, these statutory provisions have been incorporated by reference to other significant cyber laws like the *Cyber Incident Reporting for Critical Infrastructure Act*—making their reauthorization all the more critical.[5]

The aforementioned attacks demonstrate the urgent need for increased collaboration and information sharing. The expiration of these protections risks creating a chilling effect on this critical information exchange—leaving us all more vulnerable to nation-state attacks and cybercriminals moving forward. Thank you for your leadership on this important issue and we are committed to working with you to preserve these key national security authorities.

Sincerely,

Alliance for Digital Innovation
American Bankers Association
American Public Power Association
Bank Policy Institute
Business Software Alliance
Edison Electric Institute
Independent Community Bankers of America
Information Technology Industry Council
Institute of International Bankers
National Rural Electric Cooperative Association
Operational Technology Cybersecurity Coalition
Securities Industry and Financial Markets Association

---

https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf.

[3] Arielle Waldman, *CISA: BeyondTrust breach affected Treasury Department only*, TECHTARGET (Jan. 7, 2025), https://www.techtarget.com/searchsecurity/news/366617777/CISA-BeyondTrust-breach-impacted-Treasury-Department-only.

[4] Office of the Dir. Of Nat. Intelligence, *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf

[5] *See* 6 U.S.C. § 681e.