September 4, 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 fall session begins, we urge Congress to extend the September 30, 2025 expiration date for the *Cybersecurity Information Sharing Act*.[1] This bipartisan legislation, passed in the wake of the 2015 OPM breach, provides a voluntary information sharing framework that has been instrumental in strengthening our collective defense against increasingly sophisticated and severe cybersecurity threats.

Over the past ten years, the public-private communication channels established by the law have enhanced our ability to quickly respond to significant cyber incidents and mitigate associated national security risks. Moreover, because the vast majority of critical infrastructure is privately owned, the law has better positioned government partners to confront emerging cyber threats. Similarly, the law's

[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).

antitrust exemption and affiliated protections enable private companies to share cyber threat indicators—an authority cyber personnel have come to rely upon to fortify security measures and protect customer data. Consistent with the clear privacy and confidentiality expectations articulated in the law, this sharing is limited to only the actionable information security personnel need to improve cyber preparedness.

The opportunity to extend these authorities comes at a critical time. Nation-state cyber adversaries continue to target U.S. critical infrastructure and are prepositioning to conduct potentially more disruptive attacks in the future—the Salt Typhoon campaign being the latest example.[2] Federal agencies maintain volumes of sensitive information and are therefore similarly attractive targets. In the past five years alone, hackers accessed the networks of nine federal agencies during the SolarWinds incident,[3] unclassified documents at the Treasury Department during the BeyondTrust breach,[4] and most recently approximately 148,000 emails after compromising the Office of the Comptroller of the Currency.[5]

The current cyber threat landscape highlights the need for consistent public-private collaboration—of which information sharing is a central component. Without the protections codified by this statute, businesses may be less willing to share cyber threat information for fear of legal exposure. Any chilling effect on this information exchange directly benefits the nation-state attackers and cybercriminals seeking to degrade U.S. economic and national security interests. 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 Roundtable
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

[2] Aruna Viswanatha & Sarah Krouse, *Chinese Spies Hit More Than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals*, WALL ST. J. (Aug. 27, 2025), https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f.

[3] 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.

[4] 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.

[5] Letter from Rodney E. Hood, Acting Comptroller, Office of the Comptroller of the Currency, to Financial Institution CEOs (Apr. 14, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.