April 28, 2025

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

The Honorable Gary Peters
Ranking Member
Homeland Security & Governmental Affairs Committee
724 Hart Senate Office Building
Washington, DC 201510

Dear Chairman Paul and Ranking Member Peters,

The undersigned trade associations (collectively, "the associations") urge Congress to extend, for at least ten years, the *Cybersecurity Information Sharing Act* (CISA 2015), which is scheduled to expire at the end of September 2025.

Originally enacted in 2015 with broad bipartisan support, CISA 2015 established the voluntary information network to enable "public and private sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation."[1] The law remains foundational to strengthening our collective defense against cybersecurity threats, facilitating trust in the public-private partnership, and serving as the backbone of essential programs across the federal government – programs that have measurably improved the security posture of critical infrastructure in the United States and strengthened the federal governments' security awareness.

Of paramount importance, the law's antitrust exemption and liability protections enables private sector sharing of sensitive cyber information. Our nation's critical infrastructure operators depend on threat indicator sharing from one another and from the federal government to strengthen their overall defenses. A lapse in CISA 2015 authorities will curb this sharing, which is fundamental for enhancing overall awareness of national security threats.

CISA 2015 continues to improve the capacity and speed of information sharing between the private sector and the federal government, while most critically providing necessary protections for privacy and confidentiality. Illustrative of this success is the joint effort of the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) to identify the People's Republic of China (PRC) cyber actor, Volt Typhoon, in United States energy systems. This collaboration, fostered by CISA 2015, contributed to one of the most comprehensive, actionable, declassified cyber information sharing reporting in our nation's history and continues to lead to further discoveries of this advanced persistent threat actor in other critical infrastructure sectors.

[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).

Extending CISA 2015 is also pivotal for supporting the effectiveness of federal programs, like CyberSentry[2] and "Section 9"[3] support, that mutually benefit the federal government as well as the infrastructure operator. In addition, CISA 2015 plays an essential role in the functions of CISA's Joint Cyber Defense Collaborative (JCDC), which reduces cyber risk by unifying the cyber defense capabilities and actions of government and industry partners, including the associations' members. Furthermore, these statutory provisions are so undeniably indispensable that they are incorporated by reference in other significant cyber laws, including the *Cyber Incident Reporting for Critical Infrastructure Act*.[4] Within the legal framework of the industry's Cyber Mutual Assistance (CMA) Program, CISA 2015 provides CMA Program participants additional protections when sharing certain sensitive cybersecurity information with one another. These additional protections strengthen the program and enhance security for the industry by encouraging and protecting greater sharing of cybersecurity information between private entities.

For these reasons, an expiration of these protections risks leaving our infrastructure more vulnerable to cyber incidents that could impact operational integrity and resilience. The associations and the companies we represent thank you for your leadership on this issue and stand ready to engage with Congress to ensure CISA 2015 remains prioritized in reinforcing our national and energy security goals.

Sincerely,

American Fuel & Petrochemical Manufacturers Association
American Gas Association
American Petroleum Institute
American Public Gas Association
Edison Electric Institute
GPA Midstream
Interstate Natural Gas Association of America
Liquid Energy Pipeline Association

CC: The Honorable Mark Green, Chairman, House Homeland Security Committee
The Honorable Bennie Thompson, Ranking Member, House Homeland Security Committee
The Honorable Tom Cotton, Chairman, Senate Select Committee on Intelligence
The Honorable Mark Warner, Ranking Member, Senate Select Committee on Intelligence
The Honorable Rick Crawford, Chairman, House Permanent Select Committee on Intelligence
The Honorable Jim Himes, Ranking Member, House Permanent Select Committee on Intelligence

---

[2] Participating entities share threat information with CISA in real time for analysis and further dissemination to critical infrastructure operators across the nation. CyberSentry also provides valuable insights into the nature and scope of potential cyberattacks, and facilitates proactive mitigation as well as swift and effective incident response planning.

[3] *See* Executive Order -- *Improving Critical Infrastructure Cybersecurity* § 9 (February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[4] *See* 6 U.S.C. § 681e.