September 16, 2022

The Honorable Gary Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Jack Reed
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable James Inhofe
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Chairman Peters, Chairman Reed, Ranking Member Portman, and Ranking Member Inhofe:

Our associations have concerns with provisions of H.R. 7900, the National Defense Authorization Act for Fiscal Year 2023, added by amendment 554 that would require the Department of Homeland Security (DHS) to designate certain critical infrastructure as systemically important entities (SIEs). We question the amendment's ability to advance U.S. cybersecurity beyond the status quo. Among other things, the amendment would create unnecessary programmatic redundancies and put aggregated industry cyber reports at an elevated risk of exploitation by America's foreign adversaries.

Many critical infrastructure entities that are likely targets of foreign hacking campaigns want to build continuous, operationally collaborative relationships with key government agencies before crises strike. Our members believe that protecting key critical infrastructure (e.g., assets, facilities, and systems) from a significant cyberattack is a top national security priority. For several years, federal, state, and local governments and industry have embraced a partnership model to defend critical infrastructure—the majority of which is owned and operated by the private sector—from nation-state and criminal cyberattacks. This approach has been largely successful. Many focus on the unfortunate cyber incidents that occur, while too few focus on the countless cyberattacks that have been avoided.

The amendment would shift policymaking, particularly involving DHS' Cybersecurity and Infrastructure Security Agency (CISA), from being partnership driven to one that empowers CISA to impose additional cybersecurity requirements on industry. Indeed, many sectors are heavily regulated. The amendment would write into law programs that CISA administers today, such as the identification of dozens of national critical functions and the designation of SIEs as the basis of resilience-oriented risk management.

At best, the amendment would duplicate the current state of affairs. Numerous public-private partnerships are already mobilized to guard critical infrastructure from harm and

interruption. The amendment would not create any new, meaningful channels through which an SIE could work with the federal government so that national security agencies can disrupt the campaigns of threat actors on a more persistent basis.

At worst, the amendment would create potentially numerous, overlapping processes and grant CISA new authorities that may not materially improve America's cybersecurity posture. Furthermore, it would add to cyber reporting inefficiencies and pull valuable resources away from existing public-private cybersecurity programs. The amendment would shift essential business resources toward regulatory compliance as opposed to confronting cybersecurity threats.

While this list is not comprehensive of our associations' views, the amendment is of significant concern. The amendment, which passed the House without being thoroughly vetted through the regular order, is not fixable as crafted and should be rejected.

Resist Overlapping Roles and Requirements

Private sector investments in protecting our critical infrastructure are costly and must be made and used wisely. However, the amendment does not seem to contemplate how to assist mature critical infrastructure entities in ways that are truly collaborative and beneficial in defending against malign foreign cyber operations. Instead, it appears poised to replicate the ongoing work of CISA in classifying SIEs, fuel more burdensome reporting obligations and less strategic coherence, as well as reproduce important initiatives that CISA and critical infrastructure entities are currently leading.

- In 2013, the federal government established risk-based procedures to identify and designate SIEs. The amendment would create matching responsibilities at CISA and spur repetitive obligations on SIEs, many of which are extensively regulated by federal and state agencies.

- The business community is awash in existing and proposed cybersecurity and data protection disclosure/notification/reporting requirements, with no end in sight. Complicating matters, several agency rulemakings—plus the new Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) governing business reporting on cyber incidents and ransomware payments—are in their early stages and may not make effective use of industry resources.

  Also, while the amendment constructively suggests reducing duplicative reporting requirements—a role that the intergovernmental Cyber Incident Reporting Council is presently called on under CIRCIA to pursue—this goal is unlikely to be achieved. SIEs would still have to prepare many unique, time-consuming, and detailed materials for CISA.

  Private entities consider this data highly confidential and proprietary; such information, if made public, would put SIEs at a heightened risk of successful cyberattacks.

- In addition, the amendment's call for an Interagency Council for Critical Infrastructure Cybersecurity Coordination would basically copy a number of joint critical infrastructure-CISA incident response activities and policy initiatives (e.g., the development of cybersecurity performance goals) to bolster the United States' cyber preparedness.

The amendment's overlapping provisions would have real-world impacts as crucial industry resources would be forced to focus on rote regulatory compliance. Rather than passing the amendment, policymakers should help clarify the roles and responsibilities of the public sector regarding cybersecurity and streamline redundant government bureaucracy and industry mandates, not create new ones.

Pursue Operational Collaboration in the 118th Congress

Provisions in the amendment call for intelligence support to SIEs, which may seem constructive at first glance. Indeed, many in the private sector have been clamoring for actionable intelligence from the government. Unfortunately, the amendment would not stimulate the types of operationally collaborative structures between industry and national security agencies necessary to positively alter existing U.S. cybersecurity information-sharing arrangements.

- In the main, the amendment would require CISA to identify interdependencies among SIEs (e.g., common technologies and important lines of business), which has some value in cyber defense. However, as a runway to both providing SIEs with novel indicators and warnings and enabling government authorities to persistently engage hostile adversaries, the legislation would not accomplish the policymaking outcomes that sophisticated business entities need.

- Critical infrastructure entities with mature cybersecurity programs receive comparatively limited government support or actionable information to contest foreign malicious cyber activity. Notable exceptions include law enforcement. Rather than create repetitious programs, existing public-private partnerships, such as the information sharing and analysis centers and the new Joint Cyber Defense Collaborative (JCDC) at CISA, should be leveraged in more purposeful ways to degrade foreign adversaries' abilities to interfere with America's critical infrastructure.

  Nevertheless, many critical infrastructure owners and operators regularly seek opportunities for deeper operational collaboration—especially ones involving the intelligence community (IC) and national security agencies, which are permitted under U.S. law to knock our strategic adversaries off balance before they can exploit American businesses and government institutions. CISA does not undertake such operations.

- We urge Congress to prioritize and fully fund an initiative that brings together critical infrastructure and IC cybersecurity risk management experts at the Office of the Director of National Intelligence (ODNI) to better defend forward in cyberspace. Attempts have been made to address such objectives, including through the establishment of NSA's

Cybersecurity Collaboration Center and the JCDC, but optimal and consistent outcomes regarding pushing back against foreign hackers remain elusive.

An ODNI-oriented cyber program should facilitate the voluntary participation of critical infrastructure entities that opt to become increasingly significant partners of the IC. A number of critical infrastructure entities that are subjected to foreign hacking campaigns want to have ongoing, operationally collaborative relationships with national security agencies that are authorized to disrupt or halt foreign malicious cyber activity at its source.

Instead of passing the amendment, the next Congress should take a fresh look at public-private cybersecurity programs so that it can address the needs of capable critical infrastructure from a structural standpoint. Policymakers should focus on ways to improve or build upon them from the vantage point of industry sectors. Lawmakers should safeguard industry entities that voluntarily elect to take additional, tailored measures to safeguard their networks and operations based on their own assessments of risk.

Safeguard Industry Defenders

Some proponents of the amendment argue that government benefits would come with the obligations of being designated an SIE, but such gains do not appear in the legislation.

- The business community, not the government, is the main force shouldering the protection and resilience of U.S. critical infrastructure and information systems against cyberattacks led by predatory nation-state hackers and other illicit groups.

- Businesses confront relentless, often state-sponsored, cyberattacks but frequently lack effective government protection. Cyberspace is the only domain where the private sector is expected to defend itself against foreign powers and their proxies.

- Our organizations believe that this security gap justifies pairing existing and any future cybersecurity requirements with legal liability protections and express national preemption of state cybersecurity and data protection laws and requirements. These are core industry cybersecurity policy objectives that the amendment does not reflect. Greater business certainty would drive investments in better cybersecurity risk management and adherence to laws and requirements.

***

Our organizations are committed to working with lawmakers and their staffs on cybersecurity legislation. We believe that the amendment does not strike the correct balance between the cybersecurity needs of sophisticated critical infrastructure entities—which have helped develop and support many major cyber policy and legislative initiatives and are dedicating billions of dollars to protecting U.S. cybersecurity—and the policy objectives of the amendment. Striking the proper balance is crucial to the security and resilience of the United States.

Sincerely,

American Fuel & Petrochemical Manufacturers (AFPM)

American Gas Association (AGA)

American Petroleum Institute (API)

American Property Casualty Insurance Association (APCIA)

Center for Procurement Advocacy (CPA)

Consumer Technology Association (CTA)

CTIA

Healthcare Information and Management Systems Society (HIMSS)

Information Technology Industry Council (ITI)

Interstate Natural Gas Association of America (INGAA)

National Association of Mutual Insurance Companies (NAMIC)

National Electrical Manufacturers Association (NEMA)

NCTA—The Internet & Television Association

NTCA—The Rural Broadband Association

Telecommunications Industry Association (TIA)

U.S. Chamber of Commerce

USTelecom—The Broadband Association

Water Environment Federation (WEF)

cc: Members of the Senate Committee on Homeland Security and Governmental Affairs
cc: Members of the Senate Committee on Armed Services
cc: Members of the Senate Select Committee on Intelligence