CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

NEIL L. BRADLEY
EXECUTIVE VICE PRESIDENT &
CHIEF POLICY OFFICER

1615 H STREET, NW
WASHINGTON, DC 20062
(202) 463-5310

October 21, 2020

TO THE MEMBERS OF THE FY 2021 NATIONAL DEFENSE AUTHORIZATION ACT CONFERENCE COMMITTEE:

The U.S. Chamber of Commerce supports improving the situational awareness of cyber threats to more effectively protect America. We are working to advance legislative recommendations made by the U.S. Cyberspace Solarium Commission that would strengthen the cybersecurity of the business community, and the Chamber-led industry efforts to pass substantial legislation in 2015 to strengthen cooperative information sharing between the public and private sectors signify our commitment to U.S. cybersecurity.[1] Nonetheless, the Chamber believes that section 1637 of H.R. 6395, which pertains to mandated cyber incident reporting, should not be included in the final National Defense Authorization Act for Fiscal Year 2021 (NDAA).

Businesses and government entities sustain millions of cyberattacks per day. The true scope and level of impact of a detected cyber event may not be known for an extended period of time. What may be understood in the first few days of a cyber investigation can be dramatically altered by what is learned in the weeks and months that follow. Yet, as drafted, section 1637 would inject far-reaching friction and ambiguity into this process. Terms such as "covered critical infrastructure entity," "covered cybersecurity incident," and "critical infrastructure" need to be carefully crafted to prevent ineffective overreporting by industry. Creating a flood of data is not the same as generating actionable intelligence for business and government decision makers.

Incident reporting should not be an end in itself. It must address the legitimate interests of both industry and government organizations and lead to tangible consequences for malicious hackers, many of whom are sponsored by foreign powers. Similarly, the Chamber believes that section 1637 should reflect practical concerns, including liability protections for reporting by private entities, which are missing from the legislation.

There are also key compliance and cost burdens associated with section 1637, particularly workforce considerations tied to the shortage of qualified and highly skilled cybersecurity personnel in the U.S. and abroad. The Chamber believes that many policymakers share our serious concern that, if enacted, section 1637 would divert cyber professionals from their work maintaining vital systems and defending networks to comply with the legislation's rigid reporting schemes, with little appreciable gain in security across the cyber ecosystem.

[1] https://www.lawfareblog.com/cybersecurity-information-sharing-success-stories

Many regulatory structures exist with respect to incident reporting. Several critical industry sectors, such as financial services and energy, are subject to rigorous legal and regulatory obligations to report significant cyber incidents to federal and/or state agencies. It is challenging to discern what increased value would flow to the federal government when such information is seemingly already available to federal bodies.

Before adding another cybersecurity requirement on industry, the Chamber urges lawmakers to work with the business community to identity elements of section 1637 that can be mutually agreed upon. At a minimum, we contend that legislation as meaningful as section 1637 should vetted through regular order and not bypass committee consideration.

The Chamber looks forward to engaging Congress on this provision and advancing the NDAA, which is crucial to U.S. economic and national security.

Sincerely,

Neil L. Bradley