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 2, 2020

TO THE MEMBERS OF THE FY21 NATIONAL DEFENSE AUTHORIZATION ACT CONFERENCE COMMITTEE:

The U.S. Chamber of Commerce supports H.R. 6395 / S. 4049, the "National Defense Authorization Act for Fiscal Year 2021," and we ask the conferees to consider recommendations we believe would improve the overall legislation.

The Chamber supports retaining several specific, important provisions of the bill, including:

Support Codifying a National Cyber Director (NCD) - The Chamber recognizes that the House and Senate defense bills take different approaches to creating an NCD. On the one hand, S. 4049 calls on DoD and the Department of Homeland Security (DHS) to conduct an independent assessment of the feasibility and advisability of codifying an NCD. Senate lawmakers agree with the need for improved coordination of cybersecurity policy and operations across the federal government, but believe that there are additional questions that need to be answered prior to creating an NCD. On the other hand, the House bill would press forward with codifying a cyber coordinator.

The Chamber supports H.R. 7331, the National Cyber Director Act, which was added to H.R. 6395 (sections 1631–1632) in July 2020. This bipartisan bill would elevate cybersecurity decision making and coordination at the White House. It is particularly crucial that the legislation would establish the NCD as the U.S. government's senior point of contact for the American business community, which is on the front lines of cyber conflict.

The NCD would function as the administration's cybersecurity coordinator, backed with statutory authority to serve as the President's principal adviser on cybersecurity strategy and policy, review cyber budgets, and coordinate America's response to significant cyber incidents. The Chamber trusts that the codification of the NCD, which has existed in some form across several Presidential administrations, would assist the American business community in navigating federal policy initiatives and interagency processes, as well as preparing for and responding to significant cyber events. Moreover, businesses would rely on the NCD to help negotiate with federal agencies on key domestic and international cyber priorities. The NCD would send a signal to the public, including U.S. allies, that the White House prioritizes cybersecurity.

Support and fully fund the Public Wireless Supply Chain Innovation (R&D) Fund and the Multilateral Telecommunications Security (MTS) Fund - The Chamber applauds the

inclusion of the R&D Fund and the MTS Fund in S. 4049 (section 1092). These funds would promote U.S. leadership, competitiveness, and supply chain security in 5G, a critical backbone for future economic growth. The R&D Fund would provide grants to companies to develop and deploy Open RAN technologies, while the MTS Fund would support the global development and deployment of secure and trusted telecommunications in consultation with America's foreign partners.

The Chamber urges lawmakers to adopt the R&D Fund and MTS Fund authorization levels (i.e., $750 million per fund) that were included in the reported version of S. 3905, the Intelligence Authorization Act for FY 2021 (section 501) in the final FY 2021 NDAA. These spending levels would provide a critical starting point to ensure U.S. leadership in 5G. However, these funds should be replenished over time to address the long-term needs of the telecommunications industry in leveling the playing field for trusted and secure equipment worldwide.

Support continuity of the economy (COTE) legislation - The Chamber welcomes the important federal leadership provided to the business community during the COVID-19 pandemic. The coronavirus outbreak contains meaningful lessons regarding cybersecurity. The Chamber appreciates the addition of S. 3928, the "Continuity of the Economy Act of 2020," to the Senate FY 2021 NDAA (S. 4049). The Chamber is open to legislation that would call on the administration to develop a COTE economy plan to maintain and restore the U.S. economy in response to a significant cyber disruption. The Chamber believes that COTE planning and implementation activities need to be undertaken in tight collaboration with key stakeholders, including sector-coordinating councils and sector-specific agencies.

Discussions between bill writers and industry are progressing regarding necessary adjustments to the bill, including the scope of economic sectors that would be impacted ("prioritized for operation") during a major cybersecurity event. Also, the Chamber holds that legislation should reflect the conditions in which many industrial control (IC) systems operate. Computing in IC systems has converged extensively with external services, particularly information technology (IT).

The Cyberspace Solarium Commission (CSC) report calls for "parallel," or effectively analog, IC systems that are hardened to attack. However, it would be neither simple nor desirable to separate IC and IT systems, including shifting them to a parallel—or an internet-disconnected—space. The Chamber understands the desire of the CSC and bill writers to establish critical systems that are largely immune from foreign cyberattacks.

But operational and IT technologies have been converging for multiple decades, bringing remarkable efficiencies and expanded capabilities in comparison with analog systems. Instead of turning back the technology clock, policymakers should enable government agencies to partner with industry in jointly defending industrial control networks, including through the use of network segmentation.

Support strengthening the Cybersecurity and Infrastructure Security Agency (CISA) - CISA plays an increasingly critical role as the United States' risk advisor and

facilitator of alerts, tools, resources, and best practices to improve its cybersecurity position. The Chamber supports the provisions that strengthens the agency by extending the agency director's term limit to five years. This change is needed to further modernize the agency by providing stable, consistent leadership that carries out its authorities, including engaging with the business community before, during, and after cyber incidents.

Support U.S. Leadership in Artificial Intelligence - The Chamber strongly supports the inclusion of provisions that are identical or similar to Division E of the House NDAA, the National Artificial Intelligence Initiative Act, in the final conference report. These important provisions strengthens U.S. global leadership in artificial intelligence (AI) through supporting multiyear Federal investments in the AI research and development, providing for enhanced interagency coordination, facilitating the creation of a national AI research cloud, and enabling the development of AI standards including through the establishment of an AI risk management framework. The inclusion of these provisions are critical to ensuring that the U.S. can continue to innovate and responsibly develop and deploy AI systems.

Support Section 804, "Contractor Business Systems" - The Chamber supports section 804, which improves the definition for business systems and further aligns Department of Defense contracting actions with commercial sector best practices. The Chamber notes this provision was recommended by the Section 809 Panel's "Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations" and commends the Senate for ensuring consistency between the National Defense Authorization Act, the Defense Federal Acquisition Regulation Supplement, and Generally Accepted Auditing Standards.

Support Section 842, "Truth in Negotiating Act" - The Chamber supports Section 842 would establish a standard $2.0 million threshold for application of the requirements of the Truth in Negotiations Act. This provision would streamline the acquisition process, promote efficiencies, and improve acquisition timelines while eliminating administrative burdens.

Support Section 845, Commercial Sector "Best Practices" - The Chamber supports Section 845 would improve the definition for business systems and further align the Department of Defense's contracting actions within commercial sector "best practices." This provision was recommended by the Section 809 Panel's "Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations," and would ensure consistency between the National Defense Authorization Act, the Defense Federal Acquisition Regulation Supplement, and Generally Accepted Auditing Standards.

Support Section 1045, "Arctic Mission" - The Chamber supports Section 1045 would direct the Department of Defense to examine new training and equipping requirements in the Arctic. Moreover, the Chamber supports the U.S. Coast Guard's icebreaker modernization program to protect and assert U.S. national and economic security interests.

Support Nuclear Energy Leadership legislative language - The Chamber also supports retaining provisions based on **S. 903** / **H.R. 3306**, the "Nuclear Energy Leadership Act," and the associated bipartisan amendment #612 filed by Representative Luria. This legislation would facilitate revitalization of U.S. nuclear leadership through support for technology demonstrations, R&D infrastructure, fuel security, and workforce development. These activities are essential to restoring a robust civil nuclear industry and would benefit national security by

advancing nonproliferation leadership and broader U.S. geopolitical objectives while accelerating economic investment in clean energy.

Support language to strengthen and enhance critical infrastructure support from the Director of National Intelligence - The Chamber supports legislation to codify a collaborative relationship between key critical infrastructure sectors and the intelligence community. Such legislation is currently in included in Section 605 and 606 of the FY 2021 Intelligence Authorization Act, H.R. 7856. The Chamber championed the passage of the Cybersecurity Information Sharing Act of 2015, which modernized the exchange of technical threat data between industry and government bodies. However, a gap exists in U.S. cyber defenses. National intelligence capabilities to protect designated critical infrastructure, who face daily threats from hostile foreign adversaries, are needed to strengthen overall national security. This legislation would ensure that these threats are considered, prioritized, and resourced through existing intelligence community processes.

In addition, the Chamber has concerns with the following legislative provisions contained in H.R.6395 / S.4049 and would request that the committee's final product reflect these suggestions.

Oppose the cyber incident reporting amendment (section 1637 of H.R. 6395) - The Chamber respectfully opposes including the cyber infrastructure incident reporting amendment (CIIRA or the amendment) in the final FY 2021 NDAA due to process and policy concerns. Among other things, committees of jurisdiction were short-circuited by adding the amendment to H.R. 6395, the House FY 2021 NDAA (see section 1637 of H.R. 6395), without hearings or markups. Meaningful legislation such as the CIIRA should be vetted through regular order. Also, the CIIRA would violate sound cyber risk management principles and unravel the consensus that information sharing between industry and the government must be based on collaborative partnerships to work effectively.

Domestic Source Requirements - The Chamber is concerned with acquisition mandates contained in the bill, which would impose numerous changes to the conditions under which U.S. defense companies could source materials and components to support production and services. Specifically, section 822 would further restrict access to samarium, neodymium, tungsten, and tantalum for U.S. defense sector use, and section 825 would increase domestic content requirements for major military programs. As Congress is seeking to mitigate the broad economic challenges confronting the U.S., such additive compliance regimes would strain already fragile supply chains with particular impact upon small business subcontractors. Moreover, by constraining the ability of defense companies to source materials, reduced availability would raise costs and negatively affect production and delivery schedules.

Oppose Sections on Printed Circuit Boards - The Chamber is concerned with sections 826 and 830B of the House and sections 808 and 5808 of the Senate NDAA bills, which would impose new acquisition requirements on products using printed circuit boards (PCBs). These sections are intended to address perceived security vulnerabilities in the PCB supply chain. However, the Chamber is concerned these provisions would impose highly burdensome restrictions on DoD and allies and electrical manufacturers without solving the underlying vulnerabilities. The Chamber urges the Conference Committee to work with stakeholders to address these concerns before work on the NDAA is completed.

Oppose DoD and Coast Guard authority to access the equipment and information systems of operationally critical contractors (OCCs) - The Chamber urges Congress to exclude section 1635 (Expansion of Authority for Access and Information Relating to Cyber Attacks on Operationally Critical Contractors of the Armed Forces) of S. 4049 from the final FY 2021 NDAA. Section 1635 would widen DoD's authority to compel OCCs to allow DoD and/or Coast Guard access to contractors' "equipment or information" to conduct forensic analyses in the face of reported intrusions. The Chamber is sympathetic to DoD's push for this added power to mitigate cyberattacks against OCCs, but a number of questions remain unanswered.

First, there is a lack a clarity regarding the breadth of the government's access to contractor networks and systems, the role of third-party analysts, the impact of global privacy regimes, and regulatory and legal liability concerns. For example, the liability protections granted to OCCs under 10 U.S.C. section 391 do not relieve OCCs of their obligations to comply with international privacy laws, such as the EU General Data Protection Regulation (GDPR). The loss of GDPR certifications would entail considerable costs to OCCs.

Second, it would be constructive for policymakers to explain how they intend to harmonize the multiple existing and/or requested authorities in this space, including with robust input from business stakeholders. Third, last year, NDAA conferees did not adopt section 1644 of the FY 2020 Senate bill (S. 1790), which is similar to section 1635, owing to concerns with DoD's legislative proposal. The conferees directed DoD to brief Congress within 90 days after the enactment of the FY 2020 NDAA on the expected use-case for its requested authority, the expected implementation through contractual mechanisms of such authority, and how DoD is working with OCCs to secure the defense industrial base (DIB) and respond assertively to foreign cyberattacks. It's not clear what information DoD provided to the Armed Services committees and whether this influenced the legislation. The Chamber urges Congress to refrain from legislating on OCCs until stakeholders acquire more information about the results of DoD's examination and the nuts and bolts of how officials would access contractors' equipment or information and under what safeguards.

Oppose Section 1634, "DIB cybersecurity threat hunting initiatives" - The Chamber believes that the development of a government-directed DIB threat hunting program is problematic. First, we oppose including section 1634 (Defense Industrial Base Cybersecurity Threat Hunting and Sensing, Discovery, and Mitigation) of H.R. 6395 in the final FY 2021 NDAA. Section 1634 would require DoD to conduct a rapid 120-day feasibility study to launch a Defense Industrial Base Cybersecurity Threat Hunting Program (the Program). Among other challenges, the Program appears to lack sufficient upfront analyses and input from industry, especially the DIB.

Second, in contrast to section 1634, section 1632 (Assessment on Defense Industrial Base Cybersecurity Threat Hunting) of S. 4049 represents a step forward. Specifically, section 1632 would require DoD to undertake an assessment of the adequacy of threat hunting elements of the Cyber Maturity Model Certification (CMMC) program, including the need for continuous threat monitoring operations on DIB networks, prime contractors, and third-party cybersecurity vendors. But, unlike section 1634, section 1632 wouldn't necessarily trigger the creation of a DoD-administered threat hunting program.

Nonetheless, the Chamber believes that lawmakers should also push back against section 1632. There are multiple issues—such as the participation of private entities in the assessment,

the scope of a threat hunting program in the CMMC, the use of third-party assessors, the impact of domestic and international privacy rules, and legal liability concerns—that warrant additional and open consideration by bill writers and industry.

Congress should take a prudent approach to establishing a threat hunting capability in the CMMC or elsewhere. Indeed, it is widely held that the CMMC may get extended via legislation beyond Pentagon contractors to encompass civilian agencies and non-DoD contractors. The Chamber maintains that any threat hunting program must provide industry with safeguards (e.g., regulatory and legal liability protections and programmatic reciprocity), as well as facilitate the bilateral exchange of cyber threat data between government and industry. Such conditions are unclear under section 1632. The Chamber also contends that any threat reporting program would be suboptimal if it lacks methods to assess how rapidly and successfully the U.S. government is utilizing threat data to swiftly impose real consequences on malicious actors.

Oppose House language related to PFAS regulations - The Chamber urges the conferees to drop language; 1) arbitrarily banning procurement of PFAS products by DoD; and 2) expanding reporting under the Toxics Release Inventory program, effectively eliminating the TRI program's long-standing exemptions, including the de minimis threshold that ensures chemical substance quantification is practical and compliance is feasible. Both of these provisions circumvent the regulatory process under current statute.

The Chamber supports the conference agreement to H.R. 6395 / S. 4049 the "National Defense Authorization Act for Fiscal Year 2021" and we thank the conferees for their attention to our recommendations. We believe that passage of this legislation is a critical step to ensuring America's national defense commitments remain strong.

Sincerely,

Neil L. Bradley