U.S. Chamber of Commerce
Comments on Selected Cybersecurity Priorities of the FY 2021 NDAA
August 21, 2020

Reject 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.[1] 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. Additional Chamber thinking on the amendment is available here.[2]

Delay part B of section 889 (FY 2019 NDAA). For several months, the Chamber has urged Congress to extend the compliance date of section 889(a)(1)(B) of the FY 2019 NDAA—commonly known as part B—to August 13, 2021, from August 13, 2020, to bring greater coherence to the implementation of the interim rule (IR) and ensure that execution meets congressional intent.[3] Notwithstanding the Department of Defense's (DoD's) targeted, temporary waiver, which was granted by the Director of National Intelligence (DNI) until September 30, 2020,[4] the IR still applies to other executive agencies and much of industry. Most firms that do business with the government have little to no certainty about how to comply with the regulation—whose comment period does not end until September 14, 2020—owing to a hurried process.

Resetting the effective date of part B via the final FY 2021 NDAA would enable necessary improvements to section 889, while maintaining consistency with lawmakers' original aims. Further, the sweeping and complex IR leaves many issues unresolved, particularly the future breadth of the program and the definitions of certain words and phrases; the rule introduces new concepts that have yet to be fully explained.

Progress is being made on 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.

Worth highlighting, 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.[5] 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.

Codify 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. The Senate lawmakers agree with the need for improved coordination of cybersecurity policy and operations across the federal government, but they think 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 (see sections 1631–1632) in July 2020. This bipartisan bill would elevate cybersecurity decision making and coordination at the White House. What's particularly crucial, 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 the nation'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.[6]

Enact 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.[7] 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.[8]

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.[9] 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.[10]

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.

Push back on 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.[11]

Endnotes

[1] See House floor amendment #27/House Rules Committee amendment #625, which is currently section 1637 of H.R. 6395 that passed the House in July 2020.
https://armedservices.house.gov/_cache/files/f/e/feb65ce0-93fa-4985-8bd4-355238eed8d9/327A5797AA7FBB8010AFE207F75B708C.fy21-ndaa-floor-amendment-tracker-v6.pdf
https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395pcs.pdf

[2]
https://www.uschamber.com/sites/default/files/oppose_richmond_cyber_incident_reporting_amendment_fy21_ndaa_working_final_8-14-20.pdf

[3] Department of Defense, General Services Administration, and National Aeronautics and Space Administration interim rule, Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," *Federal Register*, July 14, 2020.
https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain

[4] "Pentagon wins brief waiver from government's Huawei ban," *Defense News*, August 14, 2020.
https://www.defensenews.com/congress/2020/08/14/pentagon-wins-brief-waiver-from-governments-huawei-ban

Section 889(d)(2) provides the Director of National Intelligence (DNI) with authority to grant a waiver to the head of an agency regarding the prohibitions contained in Section 889 if the waiver is in the national security interest of the U.S. The DNI's waiver authority is distinct from the authority of an agency head to provide a waiver under section 889(d)(l) and can be exercised in the DNI's sole discretion.

[5] U.S. Cyberspace Solarium Commission report, March 2020, p. 60. https://www.solarium.gov/report

[6] On July 14, 2020, the Chamber sent a letter to the full Congress urging support for H.R. 7331.
https://www.uschamber.com/letters-congress/us-chamber-letter-hr-7331-the-national-cyber-director-act

[7] Section 501 of S. 3905 refers to the Public Wireless Supply Chain Innovation Fund in S. 4049 as the Communications Technology Security and Innovation Fund.
https://www.congress.gov/bill/116th-congress/senate-bill/3905
https://www.congress.gov/116/crpt/srpt233/CRPT-116srpt233.pdf, p. 8.

See, too, H.R. 6624 the USA Telecommunications Act.
https://www.congress.gov/bill/116th-congress/house-bill/6624

[8] See the Chamber's June 25, 2020, letter to the National Telecommunications and Information Administration on the *National Strategy to Secure 5G*, especially p. 7.
https://www.uschamber.com/sites/default/files/200625_comments_nationalstrategytosecure5g_commercedept1.pdf

[9] S. Rept. 116-236 to S. 4049, the National Defense Authorization Act for Fiscal Year 2021, pp. 347–348.
https://www.congress.gov/congressional-report/116th-congress/senate-report/236/1

[10] https://www.law.cornell.edu/uscode/text/10/391

[11] For more, see the section "Establishing Metrics on Deterring Bad Actors" in the U.S. Chamber's April 2017 letter to the National Institute of Standards and Technology on the agency's proposed update to the Cybersecurity Framework.
https://www.uschamber.com/sites/default/files/final._chamber_comments_framework_v1.1_april_10_2017.pdf