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

September 29, 2020

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

The Honorable Adam Smith
Chairman
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

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

The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Chairmen Inhofe and Smith, and Ranking Members Reed and Thornberry:

Thank you for your leadership in advancing the bipartisan National Defense Authorization Act (NDAA) for fiscal year 2021. This letter follows a September 8 coalition letter the Chamber signed onto, that laid out concerns with the printed circuit board provisions in sections 826 and 830B of the House and sections 808 and 5808 of the Senate NDAA bills. We maintain significant concerns with these provisions and offer an alternate solution for your consideration.

Printed circuit boards (PCBs) are the foundation for an enormous array of electronic components, from simple products like switch boxes and radios to more complex machines like automobiles and airplanes. Their ubiquity could make them a natural target for adversaries and other malicious actors seeking to exploit or compromise them, and recent research and media reporting suggests that potential vulnerabilities could have broad impacts within the electronics industry.[1] It is important to emphasize, however, that the likelihood of such a broad-based attack is rare, even if the consequences of such an event would be significant to America's national and economic security. Accordingly, the authors of these sections are prescient in seeking to safeguard against these potential vulnerabilities.

There is, however, a more effective approach to tackling this problem. Specifically, **Congress should direct the Secretary of Defense to determine if PCB suppliers should either participate in a "trusted supplier" program[2] or adopt a design verification standard to ensure the integrity of PCBs in the supply chain**.[3] Either of these options would address the vulnerabilities contemplated in the current NDAA provisions, lessen the likelihood of damaging disruptions to supply chains and the U.S. economy, and achieve the goals articulated by the section authors.

We make this recommendation for several reasons. **First, limiting the Department of Defense's (DoD) acquisition of PCBs to the currently designated "covered countries" would result in a false sense of security.** PCBs are ubiquitous. Millions are produced and sold throughout the world each year, with vendors regularly employing third parties to acquire PCBs for specific products. There is little evidence that a malicious actor is restricted by geography. To the contrary, determined adversaries will always use every opportunity to advances their interests – anywhere in the world. No company is immune to disgruntled employees, rogue vendors, or malicious actors exploiting security vulnerabilities to insert spyware or carry out other malicious modifications. "Walling off" certain countries from providing PCBs to the DoD means that bad actors know to concentrate their efforts on PCB production facilities in "covered countries" – which these provisions do not address.

Second, these sections would prohibit major U.S. allies and partner nations (and PCB producers) from providing PCBs to DoD. Businesses located in countries such as South Korea, Malaysia, Taiwan, Vietnam, and Mexico would be prohibited from supplying products to DoD.[4] Today, approximately 12% of all PCBs are produced in South Korea, and 4% are produced in North America (including Mexico). With these nations excluded, American businesses would need to manage significant disruptions to their supply chains and risk severe PCB shortages in meeting the needs of DoD if they are unable to identify new markets to produce PCBs under the NDAA timelines.

Third, these provisions would force DoD and defense suppliers to develop cumbersome regimes to track the country of origin for an enormous array of products using a value calculation. Setting aside the difficulty that "commercial off-the-shelf" (COTS) manufacturers would have in tracking PCB country of origin by specific finished products, the more complicating barrier would be tracking the specific costs of PCB assembly. The most common way to calculate a value percentage is to use cost accounting standards, not traditionally used in the commercial marketplace, to capture PCB assembly and manufacturing material, labor, and storage costs for both covered and non-covered country of origin by finished product.

Fourth, these provisions would be challenging for producers of common, everyday products (like calculators, USB headsets, audio speakers, and desk telephones). Additional compliance regimes may be inconsistent with good risk management practices as the risk profile of these common **products is low.** In addition, these sections both use the term "national security sensitive information" which does not appear to have a standard definition in law, regulation or instruction. This could lead to a broad *ad hoc* definition that would impact systems not directly related to critical mission functions, systems, components or networks of the DoD.

It is for these last two reasons that we strongly encourage you to exclude COTS PCBs from the final provision. However, if you do include COTS, we urge you to apply this requirement in accordance with DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*. This adjustment would appropriately minimize the risk that DoD's warfighting mission capability would be impaired due to vulnerability in system design or sabotage, or subversion of a system's mission critical functions or components.

Fifth, the "trusted supplier" program or the design verification standard would address these concerns and address the underlying problem. Either of these options would allow defense contractors and commercial COTS companies the opportunity to implement a verifiable process that would provide assurances against trojan horse attacks beyond limited geographic regions for mission critical functions and components. These options would ensure the integrity of PCBs by establishing a baseline standard to verify that a PCB is not modified. This would also eliminate the need to utilize the cumbersome accounting process to calculate the value of covered and non-covered country PCBs. Companies would no longer need to provide country-centric certifications as the PCB assembly and manufacturing integrity would be verified prior to DoD acquiring a product, component or system.

The Secretary of Defense should be given the discretion to determine the most appropriate option to implement. But if DoD chooses the design standard, it should standardize the inspection process, the design hooks (or checkpoints) that enable efficient inspection, and the metrics to make this approach more effective and implementable. This would allow DoD to verify the integrity of PCBs regardless of the country of origin – and provide additional safeguards, as well. The Secretary should facilitate this process in part by working with the business community in the development of a non-government standard that satisfy defense requirements. The Secretary should also ensure the standard includes (1) a verification approach (either functional or parametric); (2) an assurance standard design that facilitates the verification process at minimal costs,[5] and which are verifiable themselves; (3) exploring emerging attacks, in particular, attacks on circuits made with nanoscale devices; and (4) developing unified trust and assurance metrics to quantify the level of confidence. The Under Secretary of Defense for Research and Engineering (R&E) should facilitate the development of this standard.

Finally, these options could be implemented in a faster time window than the current provisions – delivering a solution faster. Given that the current PCB provisions do not begin to take effect until 2023 – and would not be fully implemented until 2032 – DoD could complete and implement the "trusted supplier" program or the design standard in a faster time window, providing a solution faster than the current sections contemplate. This also would allow defense contractors and commercial COTS companies the opportunity to implement a verifiable process that would provide assurances against trojan horse attacks beyond limited geographic regions for mission critical functions and components.

We are committed to working with you on these concerns and urge you to adopt this proposal, as it would address the concerns raised by the authors of the NDAA sections in a way less disruptive to supply chains and would provide a comprehensive solution. Thank you for your consideration.

Sincerely,

Neil L. Bradley

cc: Members of the Senate Committee on Armed Services
Members of the House Committee on Armed Services

[1] "How Secure Are Printed Circuit Boards Against Trojan Attacks" by Swaroop Ghosh, Abhishek Basak and Swarup Bhunia; PCB Hardware Trojans: Attack Modes and Detection Strategies by Matthew McGuire, Umit Orgas and Sule Ozev; and "Hardware Trojan Attacks: Threat Analysis and Countermeasures" by Swarup Bhunia, Michael S. Hsiao, Mainak Banga, and Seetharam Narasimhan, July 14, 2014. Bloomberg Businessweek, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, October 4, 2018. These events in the story were strongly refuted by Tim Cook, "Apple CEO Tim Cook is continuing to call out Bloomberg's report about Chinese spy chips embedded into iCloud servers as false, proclaiming in an interview about the company's stance on privacy and taxation that the report "is 100 percent a lie." See BuzzFeed News, *Apple CEO Tim Cook is Calling For Bloomberg to Retract its Chinese Spy Chip Story*, October 19, 2018. The same article also states: "The United States Department of Homeland Security, the UK's National Cyber Security Center, NSA Senior Adviser for Cybersecurity Strategy Rob Joyce, former FBI general counsel James Baker, and US Director of National Intelligence Dan Coats have all said variously that they either have no reason to doubt the denials of the companies mentioned in the Bloomberg story or that they've seen no evidence supporting its claims."

[2] On February 13, 2019, the Institute for Printed Circuit Boards (IPC) introduced a new Qualified Manufacturers Listing (QML) program, the IPC-1791, *Trusted Electronic Designer, Fabricator and Assembler Requirements* QML, to address gaps in current electronics industry trusted supplier accreditation programs. This program provides the electronics industry with a competitive network of "trusted suppliers" to ensure a high level of integrity in the entire PCB assembly supply chain. https://www.ipc.org/ContentPage.aspx?pageid=IPC-Validation-Services-Introduces-New-Qualified-Manufacturers-Listing-Program

[3] "Trusted and Assured Microelectronics" (PE0604294D8Z) includes a PE called "645: Verification & Validation (V&V) Capabilities and standards for Trust" with one of its objectives "Physical verification, i.e., destructive analysis of integrated circuits and printed circuit boards". There was a realignment in the PB21 request, and these funds are now included in "907 / Access to State-of-the-Art (SOTA) Microelectronics – Development". In addition, the FY 2019 appropriation included Supply Chain Hardware Integrity for Electronics Defense (SHIELD), (PE 0602303E). The SHIELD program aimed to develop a technology capable of confirming the authenticity of electronic parts at any time and place. Authenticating parts or detecting counterfeit components by current means has proven expensive, time-consuming, and of limited effectiveness. An alternative solution, maintaining complete control of the global supply chain using administrative controls, can also incur substantial costs. SHIELD instead sought to incorporate a small, inexpensive silicon chip ("dielet") into the packaging of genuine components. The dielet provided unique and encrypted component identification, enabling authentication from very close proximity. Since counterfeit electronic components pose a threat to the integrity and reliability. Potential contract – Mr. *Keith Rebello*, program manager, DARPA Microsystems Technology Office (MTO).

[4] Section 36 of the AECA states the requirements for Congressional Notifications of certain defense sales and arrangements before they can be finalized– certain Foreign Military Sales cases, Direct Commercial Sales licenses, third-party transfers of equipment, and manufacturing licensing arrangements, to name a few. Section 36 also requires that offset agreements as part of certain DCS/FMS sales be disclosed to Congress. Accordingly, the PCB language is defining a qualified country as one that has a specific offset arrangement or a reciprocal defense procurement agreement that has been properly notified to Congress. According to the DFARS, South Korea is not a qualified country because they do not have a reciprocal defense procurement agreement – only a quality assurance agreement. We are currently researching Malaysia, Taiwan, Vietnam, and Mexico.

[5] "Finally, validation approaches both post manufacturing and online, can be completed with low-cost DFS solutions, which harden a design with respect to Trojan insertion or help in the validation process." See Hardware Trojan Attacks: Threat Analysis and Countermeasures. DFS = design for security. JVF1.5