U.S. CHAMBER OF COMMERCE

November 12, 2018

Via www.acq.osd.mil/dpap/dars/index.html

Linda W. Neilson
Director
Defense Acquisition Regulation System
Department of Defense
Alexandria, VA 22350

Subject: Early Engagement Opportunity—Implementation of National Defense Authorization Act for Fiscal Year 2019

Dear Ms. Neilson:

The U.S. Chamber of Commerce welcomes the opportunity to engage the Department of Defense (DoD) regarding the implementation of the National Defense Authorization Act for Fiscal Year 2019 (NDAA), particularly concerning acquisition regulations.[1]

NDAA Source Code Review Program (Sections 1654–1655): Select Points for Discussion

Sections 1654–1655 of the NDAA are two of many policy, legislative, and regulatory initiatives underway to scrutinize cyber risks to U.S. government information technology (IT) networks and systems, including those of the DoD.[2] Leading issues that the Chamber wants to discuss with DoD officials follow:

1) **Regulatory certainty.** Sec. 1655(b) of the NDAA calls on DoD to write regulations to mitigate risks to departmental systems presented by providers of IT products and services that have obligations to foreign parties. However, several businesses are currently negotiating deals with foreign entities and need clarity concerning when and how DoD intends to enforce sec. 1655. The administration and DoD should consider delaying the enforcement of sec. 1655 until a rule is written, including with input from industry stakeholders.[3]

2) **Scope of foreign parties.** The scope of foreign parties—that is, governments and "persons" that are understood to be companies in practice—is potentially so broad

[1] www.federalregister.gov/documents/2018/08/24/2018-18357/early-engagement-opportunity-implementation-of-national-defense-authorization-act-for-fiscal-year

[2] www.congress.gov/bill/115th-congress/house-bill/5515

[3] www.federalregister.gov/documents/2018/08/24/2018-18357/early-engagement-opportunity-implementation-of-national-defense-authorization-act-for-fiscal-year

(e.g., sec. 1654(a)(1) includes "activities that pose force protection" issues) that it could trigger reporting requirements that are overly broad and not necessarily oriented toward cyber threats.

3) **Review process simplicity.** A reasonably straightforward and secure process is necessary to allow foreign parties to review providers' code (possibly followed by disclosures to DoD) based on threats posed by countries of concern. Such a process requires relative simplicity and should be developed by DoD in collaboration with industry.

4) **De minimis risk reviews.** Industry typically undertakes source code reviews vis-à-vis foreign commercial partners in labs that are tightly controlled by technology companies. Such reviews generally present a de minimis risk, including to U.S. economic and national security, and thus should not automatically warrant reporting to the department. The Chamber urges DoD to provide guidance to providers concerning software assurance processes that can mitigate cyber risk and cyber threats without necessarily triggering reporting to the department.

   In addition, DoD should consider forgoing disclosure mandates if the code that has been reviewed by a foreign entity received an export license or a license exemption. The Joint Explanatory Statement (JES) suggests that an export license (exemption) should be considered equivalent to a disclosure.

5) **Disclosure responsibility.** The NDAA is not clear regarding which party is responsible for making disclosures to DoD when multiple providers share a contract with the department. For example, a subcontractor could reveal a prime contractor's code to a foreign person or government. Bill writers note that sec. 1655 intends for the disclosure obligation to fall on prime contractors. This arrangement is understandable, yet it does not account for scenarios where a prime is unaware of circumstances where its code could be revealed to foreign entities by a third party without the prime's knowledge and/or approval.

6) **Code clarity.** Industry needs DoD to clarify what code reviews are likely to be captured in the forthcoming rulemaking. On the one hand, sec. 1655(a) focuses on whether "the person has allowed a foreign government to review the *code of a noncommercial* product, system, or service … developed for the Department."

   On the other hand, the JES emphasizes whether a person "has allowed a foreign government to review or access a product *custom-developed* for [DoD] … [and] whether it has allowed a government listed in the [sec. 1654] report … to review or access the *source code* of a product [etc.] that the Department is using or intends to use. …"

   Meanwhile, the JES presses "the [DoD] Secretary to exempt from this [disclosure] requirement any product, system, or service if … [i]t is subjected only to a de minimis disclosure under *restricted access conditions*, as defined by the Secretary" [italics added].

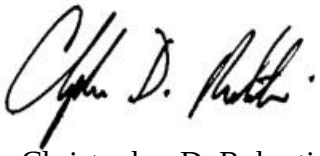
It is not clear what sec. 1655 means by source code "access," which is not defined. Typically, formal source code reviews apply if the code itself is analyzed by a person and/or a tool. But some reviews are conducted at a high level and do not get into sensitive source code material.

Clarifying what type of review is intended by sec. 1655 and the JES would enable DoD and industry to prioritize mitigating potential security risks compared with code reviews that happen under controlled conditions. Better discernment would assist vendors in understanding what code reviews should be disclosed, thus enhancing supply chain security and reducing administrative and/or reporting burdens.

***

The Chamber welcomes the opportunity to provide feedback on the NDAA, especially sections 1654–1655. We look forward to a substantive conversation between DoD and industry. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,



Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy