Telecommunications Industry Association
1320 N. Courthouse Road Suite 200, Arlington, VA 22201
703-907-7700 • tiaonline.org

December 12, 2018

Linda Neilson
Director
Defense Acquisition Regulations System
Department of Defense

Re: Early Engagement Opportunity—Implementation of Fiscal Year 2019 National Defense Authorization Act Sections 1654 and 1655

Dear Director Neilson:

The Telecommunications Industry Association (TIA) appreciates this opportunity to provide comments on implementation of the National Defense Authorization Act (NDAA) for Fiscal Year 2019.[1] While we previously provided input to the Department of Defense on Section 889, we write now to reinforce key concerns raised by other stakeholders regarding the scope and application of Sections 1654 and 1655. TIA strongly supports U.S. government action to enhance the security and resiliency of federal networks, including efforts to improve the Department's ability to manage risks to its information and communications technology (ICT) supply chain. TIA also appreciates the Department's work to improve its capabilities based on access to the best technology available. With this in mind, we urge the Department to prioritize the following areas to successfully implement Sections 1654 and 1655:

1) **Target the list of Countries of Particular Concern.**

Section 1654 directs the Secretary of Defense to create a list of countries that pose a risk to the cybersecurity of the United States to inform the scope of Section 1655's non-use and disclosure requirements. The Department should scope the criteria for inclusion on this list to include, for example, whether a country conducts or requires source code reviews and whether a country conducts cyber activities that impact U.S. cyber defenses, supply chain, or to gain unauthorized access to the intellectual property of U.S. businesses or persons. This would ensure Section 1655's requirements address risks posed by foreign government code reviews without unduly burdening U.S. businesses or diplomatic relations.

2) **Clarify the scope of code reviews.**

Section 1655 requires entities that provide a "product, service, or system … relating to information or operational technology, cybersecurity, an industrial control system, or weapons system" to notify the Department when they have allowed certain foreign actors to review the code of that technology. This requirement could be misconstrued to cover a variety of

[1] TIA is the leading trade association for the information and communications technology (ICT) industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards. Visit tiaonline.org to learn more.

Telecommunications Industry Association
1320 N. Courthouse Road Suite 200, Arlington, VA 22201
703-907-7700 • tiaonline.org

circumstances that do not pose the risk at hand if not carefully scoped. The Department should work with industry to clarify, for example, what products, systems, and services are covered, what constitutes "code review," and which foreign actors are covered by the notice requirement.

3) Clarify disclosure responsibility.

Section 1655 does not delineate which party bears responsibility for disclosures when multiple providers share a contract with the Department or when third-party software component providers may have made disclosures without the primary provider's knowledge. The Department should make clear in implementing regulations that a vendor is only responsible for notifying the Department of code reviews of which it has knowledge, provided that the vendor takes reasonable steps to maintain awareness of such activities by its partners and suppliers.

4) Establish criteria for *de minimis* code reviews.

Industry may undertake code reviews for any number of reasons and may do so in ways that do not compromise the security and integrity of the technology. To provide regulatory certainty and focus resources on high-risk code review activities, the Department should work with industry to identify criteria in which a circumstance constitutes *de minimis* disclosure.

5) Protect business confidentiality.

Section 1655 requires disclosure of sensitive and proprietary information. If made public, this could seriously harm U.S. businesses. To prevent this unintended harm, the Department should explicitly exempt information shared in required disclosures from laws requiring disclosure of information or records such as freedom of information laws. The Department should bar use of disclosed information in contract, civil or criminal actions against the disclosing company and limit access to the registry of disclosed information to federal authorities with a need to know. Similar precautions should also be taken to ensure disclosed information is not made public via the annual reports to Congress required by Section 1655.

***

TIA commends the Department's work to ensure the integrity of its supply chain, which necessitates ongoing and effective partnership with its ICT suppliers. TIA appreciates the opportunity to provide early input on implementation of the 2019 NDAA and looks forward to continued engagement as these policies continue to evolve. Please do not hesitate to contact us if our organization or membership may be of further assistance in the meantime.

Sincerely,

Cinnamon Rogers
Senior Vice President, Government Affairs
Telecommunications Industry Association