Before the
Federal Acquisition Regulation Council
U.S. General Services Administration
Washington, DC

In re: Federal Acquisition Regulation:
Prohibition on Contracting With Entities Using
Certain Telecommunications and Video Surveillance
Services or Equipment; (FAR Case 2019-009)

85 FR 53126
Docket ID: FAR-2019-0009,
Sequence No. 2

COMMENTS OF
INTERNET ASSOCIATION

Internet Association (IA) represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our companies are global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. IA appreciates the continued engagement with industry and the opportunity to provide input on the additional changes being made to the Federal Acquisition Regulation (FAR) in order to implement Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232).

IA maintains its strong support for the work being performed by the federal government to strengthen and secure our nation's infrastructure, protecting our most sensitive information and data from theft and espionage. Having developed many of the practices, policies, and procedures that are currently being used by the most secure organizations in the federal government and private sector, IA members have a clear understanding of why this effort is so important. Our collective experience in securing information and communications technology (ICT) infrastructure around the nation, including for much of the Intelligence Community (IC) and the Defense Industrial Base (DIB), also provides IA members with a unique perspective on how to successfully implement enterprise- as well as industry-wide standards.

For these reasons, and to ensure the federal government makes use of the existing knowledge related to securing hardware, software, and managed services supply chains possessed by IA members, certain aspects of the rule changes proposed in Sequence No. 2 of FAR Case 2019-009 require modification and clarification in order to ensure they achieve the intended goals of Section 889(a)(1)(B).

Update The Language In The Required Representation To Better Align With The Statute. We appreciate Sequence No.2's update to allow for an annual recertification process through the System for Award Management (SAM). This change is positive in that it will, as recognized by the FAR Council, reduce the burden on the contractor community over time. This is especially true in comparison to the offer-by-offer representation process. However, an issue with the changes outlined in Sequence No.2 mirrors that of Sequence No.1 of this present FAR Case in that there is a missing essential phrase in the representation that will be required of contractors.

As was mentioned in IA's comments on Sequence No.1, we appreciate that there was recognition of the fact that the restrictions imposed were applicable to the use of "any equipment, system, or service that uses covered telecommunications equipment or services **as a substantial or essential component of any system, or as critical technology as part of any system**" (emphasis added). However, as was true with the changes proposed in Sequence No.1, the changes proposed in Sequence No.2 are also missing this essential phrase, emphasized in the quote above.

Without the inclusion of the phrase, federal contractors face a binary choice: they must affirmatively state, under the penalty of applicable laws, that they either do or do not "use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services." In other words, the contractor must claim they know for a fact that neither they nor any of the third-party service providers they use are currently using covered equipment or services in any fashion, not just in relation to work being performed for the government.

This expansion of the applicability of the representation, going from covering "component[s] necessary for the proper function or performance of a piece of equipment, system, or service" to covering every component, regardless of how "substantial or essential" or "critical" it may be, will harm the federal government's ability to react and respond to the very same threats outlined in the Background section. Among other reasons, this is due to the fact that the type of inquiry necessary to make such an attestation will be unreasonably time-consuming, especially considering how all-encompassing it will have to be; unpredictably expensive, especially because of the breadth of no-risk or low-risk components involved in the operations of contractors of any size; impractical to carry out without the need for an "internal or third-party audit," despite assurances from the government such audits would be unnecessary; and, antithetical to the cybersecurity principles and practices already established, whether by the Cybersecurity & Infrastructure Security Agency (CISA) or the National Institute of Standards and Technology (NIST).

On that final point, CISA recognizes that "[t]he ICT supply chain is a complex, globally interconnected ecosystem that encompasses the entire life cycle of ICT hardware, software, and managed services and a wide range of entities—including third-party vendors, suppliers, service providers, and contractors." CISA's ICT Supply Chain Risk Management (SCRM) Task Force (the group expressly responsible for developing "criteria for threat-based evaluation of ICT supplies, products, and services") recognizes that there is no solution that is applicable across the entirety of the ICT supply chain and emphasizes the need for SCRM plans that address threats in accordance with their risk level. NIST's C-SCRM approach recognizes this exact same concept, stating that "[c]ost-effective supply chain risk mitigation requires agencies to identify those systems/components that are most vulnerable and will cause the greatest organizational impact if compromised," emphasizing that organizations focus on those risks rather than the entire universe of hypothetical risks.

The legislature, CISA, and NIST all recognized - threats to those components that are "substantial or essential" as well as those that are "critical" to a system are what matter most and where our resources, both in terms of human labor and capital, should be focused.

The most practical, effective, and efficient way in which to bring the implementation of Section 889(a)(1)(B) into compliance with the statute and the intent of the legislation would be to update the

representation to include the language from the statute that is already present in the FAR itself. In order to do so, the representation included in the changes proposed to paragraph (c) of FAR 52.204-26 and the changes proposed to paragraph (v)(2) of FAR 52.212-3 should be updated. Upon updating, the representation being made would then read as follows, with the requested addition in bold:

> It [ ] does, [ ] does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services **as a substantial or essential component of any system, or as critical technology as part of any system**.

This is particularly important, as the changes proposed to (a)(1) of FAR 4.2103(a)(1) and the changes proposed to the introductory text of FAR 52.204-24 reference the representation in those sections.

Finally, it is noted that existing language in FAR Subpart 4.21 actually includes the language missing from the representation. This is true for FAR 4.2101, in which "substantial or essential component" is defined, and for FAR 4.2102(a), in which the exact phrase emphasized in the paragraph above is included in both 4.2101(a)(1) and 4.2102(a)(2).

Limit Applicability Of "Use" And "Uses" To Domestic Instances Only. We reiterate the importance of limiting the applicability of Section 889(a)(1)(B) to domestic instances and reemphasize that to do otherwise would, in most cases, immediately deprive the government of standard and necessary solutions as well as those that are innovative in nature. A failure to make this modification will mean government agencies and departments with overseas operations will find it nearly impossible, if not completely impractical, to procure essential requirements that are necessary to carry out their missions.

The need for language to explicitly outline this limitation is not a theoretical or hypothetical one. In fact, as recently as September 18, 2020, only four days after the close of the comment period on the rule changes outlined in Sequence No.1, this exact scenario was acknowledged and addressed by the U.S. Agency for International Development (USAID) Section 889 Task Force in their responses to Frequently Asked Questions from their contractors about implementation of the rule. In their questions to the USAID Section 889 Task Force, contractors made clear that in some regions, the barred equipment and service(s) are provided by "a monopoly telephone/internet provider" over which the contractor has no control. This means that "[r]ealistically, there are no options" available to them, and by applicability of this rule, to the U.S. government.

Similarly, on September 11, 2020, USAID acknowledged that there is a possibility that up to 70% of their missions in Africa and 65% of their missions in Asia will be impacted, though the final results of the survey that would verify this information was still not published. This leaves a very real scenario in which U.S. efforts overseas will be severely if not entirely impossible to continue effectively while remaining compliant with this rule without a waiver. While a waiver that was issued for USAID and a handful of other agencies and departments with an expiration date of September 30, 2020 has been extended until September 30, 2022, it is still a temporary solution, as per the rule change implemented through Sequence No.1, waivers cannot be extended beyond that date without additional legislation.

Considering the language in the Benefits section states this rule is focused on stopping the efforts of the

People's Republic of China (PRC) gaining "access to the United States' sensitive technologies and intellectual property", leaving our government unable to effectively operate in Africa and Asia would be a result that is in stark contrast to the stated goals. This is a very real scenario for many of the contractors who provide food, transportation, or other basic services and necessities to support the missions and overseas efforts of the agencies and departments that depend on them, including but not limited to USAID, the Department of State (DOS), the Department of Defense (DOD), the General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA).

To that point, in the 2020 version of their Annual Report to Congress, entitled "Military and Security Developments Involving the People's Republic of China", the DOD indicates that the People's Liberation Army Navy (PLAN) presence in the African nation of Djibouti, just over 8 miles away from Camp Lemonnier (*see* Google Maps, Bing Maps), is not only expanding, but currently able to support "approximately 1 million PRC citizens in Africa and 500,000 in the Middle East" (*see* Page 48). Furthermore, in the same report, the DOD found that the PRC is seeking to build additional bases, focusing exclusively on African and Asian nations - the very same regions those USAID contractors were worried would be impacted. The DOD found that:

> ➢ The PRC has likely considered Myanmar, Thailand, Singapore, Indonesia, Pakistan, Sri Lanka, United Arab Emirates, Kenya, Seychelles, Tanzania, Angola, and Tajikistan as locations for [People's Liberation Army (PLA)] military logistics facilities. The PRC has probably already made overtures to Namibia, Vanuatu, and the Solomon Islands. Known focus areas of PLA planning are along the [sea lines of communication] from China to the Strait of Hormuz, Africa, and the Pacific Islands.
> ➢ Cambodia declined a U.S. offer to pay to renovate a U.S.-donated building on Ream Naval Base in Cambodia. Cambodia may have instead accepted assistance from China or another country to develop Ream Naval Base. If China is able to leverage such assistance into a presence at Ream Naval Base, it suggests that China's overseas basing strategy has diversified to include military capacity-building efforts. Both the PRC and Cambodia have publicly denied having signed an agreement to provide the PLAN access to Ream Naval Base.
>
> (*See* Page 129)

Without a limitation of the applicability of this rule to domestic instances or a change in the law, there is no feasible way our government could continue the current level of support and associated efforts to effectively mitigate if not eliminate the real and potential foreign threats this rule change was instituted to address. As a result, language limiting the applicability of this rule to domestic instances will be essential to its successful implementation.

In Conclusion: In Order To Achieve The Intended Goal Of Section 889, The Required Representation Must Be Modified And Limited To Apply To Domestic Use Only; Or, In The Alternative, Implementation Of The Rule Be Delayed. While a number of outstanding issues and questions remain with regards to the implementation of Section 889(a)(1)(B) through the Interim Final Rule's proposed

changes outlined in Sequence No.1, the importance of the missing language in the proposed language outlined above in the proposed changes in Sequence No.2 and its impact on the intended goals if it were applied beyond the borders of the U.S. mean this update goes beyond the necessary "administrative changes to the process of collecting information". In fact, the missing language does "affect the scope of applicability of the prohibition", as it repeats the same error in the language of the representation required of contractors present in Sequence No.1.

Without the modification to add the qualifying phrase from the statute into the required representation and ensure it applies to domestic use only, this monumental change to procurement regulations will unintentionally harm the ability of our nation's civilian, diplomatic, and military personnel to protect our nation from foreign adversaries as it will bar them from being able to effectively operate overseas. Should this modification be rejected, implementation of the rule's application to non-domestic use must be universally delayed until September 30, 2022 in order to avoid any of the unnecessary and unintended consequences that will come with inconsistent application of a rule with such broad applicability.

IA appreciates this additional opportunity to provide feedback to FAR Case 2019-009. We look forward to continuing to work with the FAR Council staff to implement this rule such that the intended objectives are achieved.