



October 18, 2018

Ms. Linda Neilson
Deputy Director, Defense Acquisition Regulations System
OUSD(AT&L) DPAP (DARS)
3060 Defense Pentagon, 3B855
Washington, DC 20301-3060

Dear Ms. Neilson:

On behalf of the leading providers of information and communications technology (ICT) hardware, software, services, and solutions to the public sector that are members of the IT Alliance for Public Sector (ITAPS),¹ we appreciate the opportunity to provide early input on the implementation of sections included in the National Defense Authorization Act (NDAA) for Fiscal Year 2018 published in the Friday, August 24, 2018 *Federal Register*.

ITAPS shares the government's interest in protecting our digital information and systems through improving the security of ICT supply chains and appreciates the opportunity to share our perspectives on Section 889, Prohibition of Certain Telecommunications and Video Surveillance Services or Equipment; Section 881, Extension of Supply Chain Risk Management Authority; and, Sections 1654-55, Disclosure of Information Regarding Foreign Obligation, as adopted in the FY19 NDAA.

Our companies work to secure the technology systems that government, citizens and corporations use to improve their missions, lives and businesses and the digital infrastructure our economy depends upon for unprecedented opportunities and prosperity. The protection of our customers, our brands, and our intellectual property – which are the essential components of our business – is critical to our ability to grow and innovate in the future. As such, we seek to maintain the highest levels of integrity in our products and services. ITAPS members have complex supply chains reaching across multiple countries, from which these products and services are developed, manufactured, assembled, and distributed across the globe. Our members understand the imperative for deep involvement in establishing successful supply chain security practices and that it is critical to maintain the highest levels of integrity in products and services, regardless of whether they are sold or who the customer may be.

We believe strongly that there is a need to discuss how the private sector and government can work together to address evolving supply chain threats our nation faces and how a public-private partnership is necessary to protect our nation's critical infrastructure and digital economy. We request the government take aggressive efforts to survey and capture industry perspectives as regulations to implement these provisions are developed. We also strongly reiterate a long-standing request from the tech sector to receive, to the maximum extent practical, a briefing to share information about the threat and vulnerabilities so that companies, and the sector as a whole, can work with the Department to effectively mitigate risk and liability.

We submit the following questions and comments as matters of the utmost urgency to federal government contractors and their subcontractors and suppliers in this dialogue and suggest they can serve as a starting point for such a dialogue and engagement with industry. All of these provisions will have a significant impact on our member

¹ **About ITAPS.** ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology [companies](#) building and integrating the latest innovative technologies for the public-sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter [@ITAlliancePS](#).

company's product offerings, business models and supply chains and have garnered the attention of senior corporate executives in order to understand the liabilities these proposals can create. More importantly, these provisions pose grave consequences for the Department's mission, and, specifically, the ability to inform and support the warfighter, if they are implemented in a fashion that does not effectively balance the need for security with the desire to inject innovation into the national security mission. We look forward to working with you to find the proper balance.

FAR Case 2018-017, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment Implements.

Section 889 of the FY19 NDAA prohibits the procurement of covered equipment and services from Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Technology Company or Dahua Technology Company, to include any subsidiaries or affiliates. We believe it is important for industry and government to work together to provide clarity on the scope of application of this provision across business enterprises and geographies. It is also critical that we jointly identify and employ a common taxonomy to assure that concerns are understood and addressed by all stakeholders.

For Section 889(2)(B), consideration should be given where a system which includes covered equipment, but that has by design or implementation mitigating controls that block routing or redirection of user data traffic. The language currently provides that *nothing in paragraph (1) shall be construed to—“ ... (B) cover telecommunications equipment that cannot route or redirect user data traffic”* which doesn't take into consideration a common security approach where equipment or systems (or the network they reside in) have additional mitigating security controls (ex. air gapped network, data diode, firewalls, etc.) that block routing or redirection of user data traffic. Without this additional consideration NDAA could inadvertently sweep into the prohibition systems that are secure.

Of equal importance, Section 889 does not define several key terms. For instance, subsection (a)(1)(A) prohibits agencies from procuring or obtaining covered equipment or services, and subsection (a)(1)(B) prohibits the government from entering into or extending contracts with an entity that “uses 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.” ITAPS believes the key question is whether “use” is limited to the context of the performance of specific federal contracts. Such a limitation makes compliance with these prohibitions far more manageable across global business enterprises and limits application to covered equipment and services used by private entities under contract with executive agencies (or 3rd parties using federal grants and loans). The Department should make it clear that such “use” provisions apply only in the context of performance of federal contracts to avoid confusion, unintended compliance exposure, and harm to the U.S. government's supply chain of secure service providers. Without such a clarification, there is a risk that the broad statutory authority could be read to prohibit procurement with reliable contractors that used covered equipment in other settings unrelated to a federal contract; e.g., mere use of a camera in an unrelated setting (such as a warehouse) should not disqualify that contractor from all business with the federal government. Such an outcome would be inconsistent with the national security objectives of the control and could lead to a lack of U.S. government access to essential mission support capabilities.

Similarly, we also believe the exclusion included in subsection 889(a)(2) must realistically be interpreted with the reality that in some parts of the world the listed companies have extensive, and in some cases exclusive, penetration for their products or the services they enable. Consequently, the prohibition of subsection (a)(1)(A) must be read and implemented to be limited to the United States and its territories. Conversely, should the

prohibition on contracting with entities that “use” covered equipment or services amount to a broader exclusion it could lead to a lack of access to even essential mission support capabilities both inside and outside of the United States and an inability to innovate in any meaningful way.

We also point to the need for further definition regarding the phrase “an entity owned or controlled by, or otherwise connected to, the government of the People’s Republic of China.” It is unclear what business and corporate relationships may be covered. For example, does this cover joint ventures or partnerships companies have established to obtain market access into China? While we understand concerns such business relationships may create, it is frequently a business imperative in order for an American technology company to be able to offer their goods and services to the largest marketplace in the world. We believe that there is a balance between these concerns and the economic and market realities and suggest the Department look at how similar terms are defined by the Departments of Commerce and Justice and the National Aeronautics and Space Administration to implement Section 515 of the Commerce, Justice, Science Appropriations bill. Furthermore, the terms “essential, substantial or critical technology” are undefined. It is imperative to the success of any implementation that the Department and industry work to identify common taxonomy and definition to clarify these specific terms and phrases in order to effectively sustain mission programs and support, attract innovation for national security needs and allow manufacturers and developers the ability to identify new suppliers and modify or transition their offerings.

Finally, we would also draw attention to the terms “equipment” and “produce.” It might behoove the Department to view potential definitions that exist in current regulations (such as export regulations in 22 C.F.R. § 120.45 (ITAR), etc.). Finding consistencies in existing regulations that share similar security goals should aid compliance and help facilitate discussion.

DFARS Case 2018-D064 Disclosure of Information Regarding Foreign Obligations

Sections 1654- 1655 of the FY19 NDAA requires certain offerors and contractors to disclose foreign obligations. As with Section 889, key terms are undefined in the language of the provision. Terms that should be the focus of such efforts to frame a taxonomy and bring clarity include “foreign person, obligation or review and access.” The language as constructed could reach even the COTS process and incidental development thereto. Depending on the outcome of such a discussion, this rule could have a broad or narrow impact on ICT companies and create substantial liabilities for companies in the industrial base that do business with the Department.

We strongly believe that instead of prohibiting software that may have a connection to China or other U.S. cyber adversaries, the Department should focus on adopting effective mitigation strategies that address risks which can originate from foreign spying or sabotage to insider threat. We also believe that the provision should clarify due process mechanism, for instance, a means for appealing mitigations measures that would exclude a vendor from the market. In addition, although we applaud the legislation’s efforts to assure uniform application of the Freedom of Information Act (FOIA), it would be very helpful for regulations to clarify unequivocally that existing FOIA protections, notably, the right of the owner of information to defense against what it perceives to be the improper release of its information (propriety or not), is not changed in the new regime. Likewise, we believe that the implementation of the provision should include confidentiality requirements for submitted information and mitigation deliberations to prevent exposure of vulnerabilities and the creation or expansion of risks and liabilities for the mission and the supply chain, and otherwise to allow vendors to assist in mitigation efforts expeditiously. Finally, we believe that any implementing regulatory regime should recognize and promote standards for sufficiency of existing corporate software assurance regimes. Many companies utilize such regimes whose requirements, like

corporate home country reviews with no external equipment and other security protocols, that could help facilitate, if not expedite, the Department's mitigation efforts.

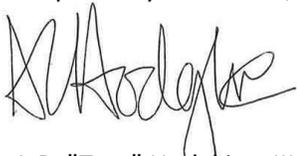
DFARS Case 2018-D072 Extension of Supply Chain Risk Management Authority Implements

Section 881 of FY19 NDAA repeals Sections 806(g) of FY11 NDAA and 806(a) of FY13 NDAA making the authority permanent. Section 881 also provides updated definitions related to Supply Chain Risk. We remain concerned about the inability of companies to receive notice about risks in their supply chains and the opportunity to mitigate the risk. The Department should be required to develop a mechanism to share these risks without disclosing methods and sources, so companies can take necessary actions to mitigate or eliminate them. Any risk severe enough to trigger exclusion is too harmful to be left unmitigated to cause further damage to the defense industrial base and the America economy. It would be grossly irresponsible to do anything less.

Along the same lines, it is especially challenging to plan for, and assist with, the Department's risk mitigation efforts in the face of constant change arising from multiple supply chain-related legislative and regulatory initiatives. It would be in the interest of all stakeholders for the Department to reach out to policymakers and support the coordination of initiatives to facilitate consistent, efficient, and effective supply chain risk mitigation.

Thank you again for requesting our input on these important regulatory matters, and for your consideration. Should you have questions, please contact Pamela Richardson Walker at pwalker@itic.org.

Respectfully submitted,



A.R. "Trey" Hodgkins, III, CAE
Senior Vice President, Public Sector

Cc: Emily Murphy, Administrator, General Service Administration
Lesley Field, Acting Administrator, Office of Federal Procurement Policy
Ron Ross, National Institute of Standards and Technology