The Year in Review

Volume 54 *International Legal Developments Year in Review: 2019*

Article 14

February 2024

International Procurement

Eric P. Roberson

THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

International Procurement

ERIC P. ROBERSON[1]

This article reviews international law developments in the field of international procurement in 2019.

I. Recent Developments in Securing U.S. Government Networks and the Supply Chain: Regulators Implement Annual Defense Legislation That Takes Aim at Foreign Companies

Building upon the prior year's annual defense authorization act, the U.S. Congress, via the National Defense Authorization Act of 2019 (2019 NDAA), has again taken aim at foreign companies suspected of having close ties to certain U.S. foreign adversaries, especially China. Earlier this year, regulators implemented the 2019 NDAA, which is among the most recent efforts by the U.S. Government to secure its networks and procurement supply chain. The 2019 NDAA and its implementation in the Federal Acquisition Regulation (FAR), as well as other complementary mechanisms focusing on network and supply chain security, are discussed below. Also discussed below are additional initiatives that may be on the horizon and would likely impact foreign companies doing business with the U.S. Government.

A. THE 2019 NDAA

Citing national security concerns, the 2019 NDAA effectively cut off access to the U.S. Government marketplace to two Chinese companies, Huawei Technologies Co., Ltd. (Huawei) and ZTE Corp. (ZTE).[2] Notably, the 2019 NDAA builds upon action already taken against Huawei and ZTE,[3]

1. Section I, "Recent Developments in Securing U.S. Government Networks and the Supply Chain: Regulators Implement Annual Defense Legislation That Takes Aim At Foreign Companies," was drafted by Eric P. Roberson, a Managing Associate in the Denver, CO office of Dentons US LLP where his practice covers a wide range of government contracts matters. Mr. Roberson also served as the editor of the International Procurement Committee's Year in Review for 2019. The views of the author and editor are not attributable to his law firm. The article covers developments during 2019. For more information about the International Procurement Committee *see International Procurement Committee*, ABA, https://www.americanbar.org/groups/public_contract_law/committees/international/ (last visited June 3, 2020).

2. John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., § 889, 132 Stat. 1636 (2019 NDAA).

3. Similarly, in the case of Huawei and ZTE, the 2018 NDAA prohibited DOD from procuring telecommunications equipment or services from Huawei or ZTE to carry out nuclear deterrent or homeland defense missions that use "covered telecommunications equipment or

as set forth in the 2018 NDAA.[4] The 2018 NDAA also restricted certain products developed by Russian cybersecurity company, Kaspersky Lab, Inc. (Kaspersky).[5] The 2019 NDAA broadened the restrictions on the U.S. Government's procurement of telecommunications equipment or services from Huawei and ZTE. The 2018 NDAA restrictions were limited to nuclear deterrent or homeland defense missions carried out by the U.S. Department of Defense (DOD).[6] The 2019 NDAA extended the 2018 restrictions to all executive agencies and essentially for all other purposes, i.e., the prohibition was no longer limited to nuclear deterrent and homeland defense missions.[7]

In addition, the 2019 NDAA barred executive agencies from entering into contracts with any company 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."[8] Further, the 2019 NDAA authorized the Secretary of Defense to extend such prohibitions to additional entities where the Secretary "reasonably believes [such] an entity [is] owned or controlled by, or otherwise connected to, the government of [The People's Republic of China]."[9]

1. *Implementation of the 2019 NDAA*

On August 13, 2019, the DOD, the U.S. General Services Administration, and the National Aeronautics and Space Administration issued an interim rule establishing two new contract clauses in the FAR. Specifically, section 889(a)(1)(A) of 2019 NDAA (Interim Rule) is implemented by FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment,[10] and FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.[11]

---

services as a substantial or essential component of any system, or as critical technology as part of any system." John S. McCain National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong., § 1634, 131 Stat. 1283 (2018 NDAA).

4. *Id.* § 1634.

5. Specifically, the 2018 NDAA prohibited any U.S. Federal agency from using "any hardware, software, or services developed or provided, in whole or in part, by (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership." *Id.* § 1656.

6. H.R. 2810 § 889.

7. H.R. 5515 § 889(a).

8. *Id.* §§ 889(a)(1)(B), 889(b) (The 2019 NDAA also prohibits loan and grant recipients from federal funding unless they agree to comply with the prohibitions).

9. *Id.* § 889(f)(3)(D).

10. Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, FAR 52.204-24 (2019).

11. Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, 84 Fed. Reg. 40216, 40216 (Aug. 13, 2019) [hereinafter Prohibition on Contracting]; *see* Complaint, Huawei Techs. USA, Inc. v. U.S., No. 4:19-CV-159, 2020 WL

This Interim Rule became effective immediately upon its publication. As explained above, these clauses prohibit executive agencies from procuring "any equipment, system[,] or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system."[12] Notably, these restrictions apply to prime contractors and subcontractors throughout the supply chain.[13]

At a high level, FAR 52.204-24 requires an offeror to submit a representation identifying any "covered telecommunications equipment or services" to be provided under a contract.[14] The Interim Rule also contemplates that this certification will be included in the annual representations and certifications made via the System for Award Management.[15]

Similarly, FAR 52.204-25 in sum provides that contractors are expressly prohibited from providing any equipment, system, or service that uses covered telecommunications as a substantial or essential component of any system, or as a critical technology as a part of any system unless an exception or waiver applies.[16] Additionally, contractors must submit a report in the event that a contractor discovers use of covered equipment or services during the performance of a contract within one day of discovery.[17] A follow-up report is due within ten days after the initial report.[18]

2. *Compliance, Considerations, and Challenges*

The implementation of the Interim Rule has immediate and wide-reaching implications. Huawei is one of the world's largest manufacturers of telecommunications equipment.[19] As such, the restriction on contracting with a company that uses covered equipment as part of a substantial or essential component of any system, or as a critical technology as a part of any system, has the potential to impact a significant number of domestic and foreign companies doing business with the U.S. Government.

805257 (E.D. Tex. Feb. 18, 2020) (Huawei challenged the validity of the 2019 NDAA's broad prohibition in U.S. district court prior to the issuance of the Interim Rule); *see* Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 909 F.3d 446, 453 (D.C. Cir. 2018) (Huawei's challenge follows a similar challenge initiated by Kaspersky on the prohibition of Kaspersky products as set forth in the 2018 NDAA. The D.C. Circuit denied Kaspersky's challenge and Huawei's case is currently pending at the U.S. District Court of the Eastern District of Texas).

12. FAR 52.204-24(b).

13. *See* FAR 52.204-25(d), (e) (2019); Prohibition on Contracting, 84 Fed. Reg. at 40,218.

14. FAR 52.204-24 (2019).

15. Prohibition on Contracting, 84 Fed. Reg. at 40,219.

16. FAR 52.204-25(b) (2019).

17. FAR 52.204-25(d)(2)(i) (2019).

18. FAR 52.204-25(d)(2)(ii) (2019).

19. Jonathon Weber, *Explainer: What Is China's Huawei Technologies and Why Is It Controversial?*, REUTERS (Dec. 6, 2018), https://www.reuters.com/article/us-usa-china-huawei-explainer/explainer-what-is-chinas-huawei-technologies-and-why-is-it-controversial-idUSKBN1O5172.

Matters are further complicated by the lack of clear definitions of key contractual terms: while the term "critical technology" is more precisely defined, the terms "substantial" and "essential" are not.[20] This lack of clarity will likely create tension and confusion for affected companies, especially where an executive agency determines that the use of covered equipment rises to the level of "substantial" and "essential." While the government is authorized to waive the restrictions imposed by the 2019 NDAA, it will likely be difficult to get the government to agree to a limited waiver because of the national security concerns involved.[21] As such, any representation to the government that a company is using covered equipment will likely present itself as a significant obstacle to satisfying the government's requirements or demonstrating compliance. Accordingly, if the government determines equipment is covered by the Interim Rule, contractors may lose significant government business. In the event of noncompliance, contractors could also face contract termination, suspension, and debarment, as well as liability under the False Claims Act.

These compliance problems are compounded by the lack of clarity on what equipment is actually covered by the rule. For instance, the Interim Rule does not clearly state the specific type of equipment that is banned. Additionally, it requires contractors to avoid obtaining such equipment from "subsidiaries or affiliates" of Huawei, ZTE, and other named Chinese manufacturers even though ascertaining the identity of such subsidiaries and affiliates may be prove quite difficult.[22] Indeed, such obligations will require a company to undertake costly and time-consuming compliance activities to independently verify whether the products they use are linked to a prohibited source.

Moreover, the Interim Rule also imposes a challenging reporting requirement of a single business day to inform the government that equipment covered by the rule has been discovered. It remains to be seen if the Government will modify the Interim Rule to provide an additional amount of time to perform an adequate investigation and to appropriately assess that any equipment discovered is in fact covered by the rule.

B. Other Mechanisms Addressing Network and Supply Chain Risk

In addition to the 2019 NDAA (and other authorities not discussed here), the U.S. Government has several other mechanisms available that seek to

20. *See* FAR 52.204-25(a).

21. *See* FAR 52.204-25(b) (2019); FAR 4.2104 (2019).

22. For example, it is unclear whether a self-certification by a supplier is sufficient or what level of independent diligence will be necessary to demonstrate compliance. Even then, it is not readily apparent that any independently verifiable information regarding corporate ownership of an entity will be readily accessible or available. *Cf.* U.S. Gov't Accountability Office, *Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership*, GAO-20-106, 35–37 (Nov. 2019) (noting the difficulty in identifying and verifying contractor ownership).

address cyber and supply chain risks presented by foreign-owned companies, several of which are briefly discussed below.

1. *The U.S. Department of Commerce "Entity List"*

Under the Export Control Reform Act (ECRA), the Secretary of Commerce is required to "establish and maintain a list of foreign persons and end-uses that are determined to be a threat to the national security and foreign policy of the United States."[23] Once an entity is placed on the Entity List, a company is subject to specific license requirements for the export or transfer of specified items.[24] Thus, a company placed on this list would need to obtain a license from the Bureau of Industry and Security before obtaining these items that are subject to the U.S. Department of Commerce's (Commerce) export and transfer restrictions.[25] The placement on this list could effectively result in the "death penalty" of the named company.[26] Indeed, Commerce initially placed Huawei (and many of its non-U.S. affiliates) on the Entity List on May 21, 2019, and has recently granted another temporary reprieve, pending final review.[27]

2. *Presidential Executive Authority Regarding National Emergencies*

Additionally, aside from the authority provided by the ECRA, the President is also vested with broad authority to declare national emergencies, impose restrictions on foreign companies, and may exclude such companies from the U.S. marketplace under the International Emergency Economic Powers Act (IEEPA).[28] Notably, under the IEEPA, the President is authorized to declare a national emergency and issue an executive order prohibiting U.S. citizens from entering into transactions related to persons and property subject to such orders.[29]

3. *FAR and DFARS Clauses*

In addition to the Interim Rule discussed above, the Defense Federal Acquisition Regulation Supplement (DFARS) already restricts certain purchases from a broad category of Chinese companies. Specifically, DFARS 252.225-7007 prohibits DOD from acquiring by contract or

23. H.R. 5515 Subtitle B (codified at 50 U.S.C. § 4813(a)(2)) (ECRA).
24. *See* 15 CFR § 744.11.
25. *Id.*
26. *See* Felicia Sonmez, *Commerce Department Will Extend Huawei Reprieve, Ross Says*, WASH. POST (Aug. 19, 2019), https://www.washingtonpost.com/politics/commerce-department-will-extend-huawei-reprieve-ross-says/2019/08/19/82a11436-c275-11e9-9986-1fb3e4397be4_story.html.
27. Addition of Entities to the Entity List, 84 Fed. Reg. 22,961 (May 21, 2019); Shannon Bond, *U.S. Firms Get 90-Day Extension to Work with Huawei on Rural Networks*, NPR NEWS (Nov. 18, 2019), https://www.npr.org/2019/11/18/780473704/u-s-firms-get-90-day-extension-to-work-with-huawei-on-rural-networks.
28. 50 U.S.C. § 1701.
29. *Id.*

subcontract—at any tier—items covered by the United States Munitions List or the 600-series of the Commerce Control List from any Communist Chinese Military Company.[30] While this clause does not name specific entities like the Interim Rule, a Communist Chinese Military Company is broadly defined as any entity, regardless of geographic location, that is (1) a part of the commercial or defense industrial base of the People's Republic of China (including a subsidiary or affiliate of such entity); or (2) owned or controlled by, or affiliated with, an element of the Government or armed forces of the People's Republic of China.[31]

C. Other Initiatives on the Horizon

Notably, there are a number of additional U.S. Government initiatives aimed at enhancing network and supply chain security, several are briefly summarized below.

1. *National Defense Authorization Act for Fiscal Year 2020*

Congress is considering prohibiting mass transit agencies from using federal transit funds to purchase rail cars from manufacturers "owned or controlled by, is a subsidiary of, or is otherwise related legally or financially to a corporation based in" certain countries, including China.[32] Also under consideration are limitations on the removal of Huawei from the Entity List.[33]

2. *Secure and Trusted Communications Networks Act of 2019*

This bill seeks to prohibit Federal funds from being used to purchase certain communications equipment or services posing national security risks.[34]

---

30. Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies, 48 C.F.R. § 252.225-7007 (2018).

31. *Id.* § 252.225-7007(a); *See* FAR 52.204-21 (in addition, there are number of other FAR and DFARS clauses that focus on securing government data, information systems, and the supply chain that complement the FAR interim rule); Safeguarding Covered Defense Information and Cyber Incident Reporting, 48 C.F.R. § 252.204-7012 (requiring that covered contractors implement certain security controls to safeguard certain types of information that reside on or transit or processes, stores, or transmits such information through a covered information system.). Notice of Supply Chain Risk, 48 C.F.R. § 252.239-7017 (2019); Supply Chain Risk, 48 C.F.R. § 252.239-7018 (2019) (focusing on supply chain security and permitting the agencies to "consider information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain" prior to contract award and during performance).

32. National Defense Authorization Act for Fiscal Year 2020, H.R. 2500, 116th Cong., § 896 (2019) (2020); *see also* Off. U.S. Trade Representative, Special 301 Report (Apr. 2019).

33. H.R. 2500 § 1250D.

34. Secure and Trusted Communications Networks Act of 2019, H.R. 4459, 116th Cong. (2019).

3. Securing the Homeland Security Supply Chain Act of 2019

This proposed legislation seeks to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to implement certain requirements for information relating to supply chain risk when carrying out certain procurements.[35]

4. Proposed Department of Commerce Rule on Supply Chain Risk[36]

The Department of Commerce proposed the implementation of regulations that govern the processes the Secretary of Commerce will use to identify, assess, and address certain information, communications technology, and service transactions that pose an undue or unacceptable risk to critical infrastructure, digital economy, U.S. national security, or the safety of U.S. citizens. Comments were due December 27, 2019.

35. *See* Securing the Homeland Security Supply Chain Act of 2019, H.R. 3320, 116th Cong. (2019).

36. *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316 (Nov. 27, 2019).

THE YEAR IN REVIEW

AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW