

INTERNATIONAL BUSINESS ALERT

JUNE 12, 2020

YUANYOU (SUNNY) YANG

412.235.1484

yyang@porterwright.com

What you need to know about Section 889 compliance as we move closer to the August 2020 implementation deadline

A major portion of the sweeping [John S. McCain National Defense Authorization Act for Fiscal Year 2019](#) (NDAA) that impacts federal contracts will take effect in August. Section 889 prohibits the federal government from directly procuring “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 a part of any system” or *entering into a contract with any entity that uses such covered telecommunications equipment or services*. The legislative text required that section 889(a)(1)(A) and 889(a)(1)(B) be implemented one and two years following enactment of the NDAA, respectively. Section 889 is far reaching and extremely broad, Section 889(a)(1)(A) requires federal government contractors to certify to the U.S. government that any equipment, system or service it supplies to the U.S. government is devoid of any equipment or services from those banned Chinese technology or surveillance companies, and Section 889(a)(1)(B) further requires federal government contractors to certify to the U.S. government that their entire global supply chain, not just the part of the business that contract with the U.S. government, is devoid of equipment, system or service from those banned Chinese technology or surveillance companies.

Section 889(a)(1)(A) went into effect on Aug. 13, 2019. Section 889(a)(1)(B) is statutorily required to be implemented by Aug. 13, 2020.

Regulatory language has yet to be published, leaving a lot of uncertainties, particularly for small businesses as the country is still coping with the massive impact of COVID-19. It applies to all kinds of federal contracts, from healthcare to information technology, from aerospace

This law alert is intended to provide general information for clients or interested individuals and should not be relied upon as legal advice. It does not necessarily reflect the views of the firm as to any particular matter or those of its clients. Please consult an attorney for specific advice regarding your particular situation.

Please see our other publications at www.porterwright.com/media.

to automotive, from semiconductor to defense industry, and could implicate almost all companies that has any contractual relationship with the U.S. federal government, including global subsidiaries and service providers far away from the company's supply chain. As we are approaching the implementation deadline in two months, aerospace, information technology, car manufacturing and a dozen other industries that will be impacted most have engaged in lobbying to seek more time for compliance. It also becomes increasingly important that companies understand the scope of Section 889, engage in lobbying efforts it deems necessary, and take proper measures immediately to ensure compliance.

Section 889 background and legislative development

The [NDAA](#) was signed into law on Aug. 13, 2018 and imposed new restrictions on procurements for telecommunications equipment or services based on ties to certain Chinese entities, thereby growing the list of forbidden products for federal contractors. Specifically, Section 889(a)(1) prohibits executive-branch agencies from initiating procurements or entering into contracts for certain telecommunications equipment or services from companies associated with, owned by, or controlled by China (part A), that are to be used "as a substantial or essential component of any system, or as critical technology as part of any system" (part B). Part A requirements took effect on Aug. 13, 2019, and Part B will take effect on Aug. 13, 2020. Section 889(b)(1) also prohibits the federal government to use loan or grant funds to procure or enter into contracts for certain telecommunications equipment or services from companies associated with, owned by, or controlled by China.

The U.S. Department of Defense (DoD), the U.S. General Services Administration (GSA) and the U.S. National Aeronautics and Space Administration (NASA) jointly hosted a [public meeting](#) to obtain views from experts and interested parties regarding implementation of Section 889 on July 19, 2019. Following that meeting, the Federal Acquisition Regulation (FAR) Council released an interim rule, [Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment](#), on Aug. 13, 2019, implementing these restrictions in accordance with Section 889(a)(1)(A) of the NDAA. The initial interim rule created a new [FAR Subpart 4.21](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, as well as two new contract clauses, [FAR 52.204-24](#), Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, and [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, all of which went into effect Aug. 13, 2019.

Concurrent with the release of the FAR interim rule, the Office of the Under Secretary of Defense issued the [Memorandum re DoD Procedures Implementing FAR 4.21, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment](#) (FAR Case 2018-017) (Aug. 13, 2019), laying out DoD procedures to implement the prohibitions contained therein. These procedures apply to contracts,

task orders, and delivery orders, including basic ordering agreements (BOAs), orders against BOAs, blanket purchase agreements (BPAs), and calls against BPAs. The DoD memo mandates the contracting officer to include the new clauses and requirements in any new solicitations, orders, modifications or exercises of options after Aug. 13, 2019.

Additionally, the GSA issued the [Memorandum for GSA Contracting Activities: FAR and GSAR Class Deviation – Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment](#) (Aug. 13, 2019). The GSAR Derivation removed the order-level representation obligation for certain low-risk Schedules. But the deviation leaves in place the contract-level representation. The GSA further issued [Guidance on Section 889 FAR Rule](#) and [889 Deviation FAQs](#).

On Sept. 9, 2019, the GSA announced it would be issuing a [mass modification](#) requiring all new and existing GSA Multiple Award Schedule (MAS) contracts to include two new clauses. The two clauses to be added to all MAS contracts are:

- FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, and
- GSAR 552.204-70, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment

MAS contractors will have 60 days from the date the modification is issued to accept the modification by incorporating the above clauses into their Schedule contracts and providing the representation required by GSAR 552.204-70. Additionally, MAS contractors must accept this modification prior to exercising their contract's next option period, and the GSA may cancel contracts if the contractor has not accepted after the 60-day period.

On November 6, 2019, the GSA hosted an [Industry Engagement Meeting](#) to discuss how Section 889 of the NDAA will affect GSA's business and supply chain. Many questions from the attendees at the industry forum, however, suggest that the industry still has not come to grips with the scope of the forthcoming rule. Several of the other panelists at the Industry Forum expressed concern over the impact of the rule (both part A and part B) on small businesses as well.

On Dec. 13, 2019, the FAR Council issued a second interim rule implementing Section 899(a)(1)(A) of the NDAA, [Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment](#) (84 Fed. Reg. 68314). The portion of the initial interim rule memorialized in [FAR 52.204-24](#) that required a new certification in every offer was apparently found to be unduly burdensome. Instead, the second interim rule aims to reduce the burden on the contracting community by allowing an offeror to represent annually through the System for Award Management (SAM), via SAM.gov, whether it provides covered telecommunications equipment or services. The new annual representation, [FAR 52.204-26](#), requires

an offeror to represent whether it does or does not “provide covered telecommunications equipment or services as part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.” This interim rule will reduce the burden on offerors that do not provide covered telecommunications equipment or services by eliminating the need to complete [FAR 52.204-24](#) in response to every offer. The second interim rule took effect immediately on Dec. 13, 2019, but comments were due by Feb. 11, 2020.

On Jan. 22, 2020, the U.S. Office of Management and Budget (OMB) issued a [proposed rule](#) to its grants and agreements regulations at Title 2, Part 200 of the Code of Federal Regulations, Subtitle A-OMB Guidance for Grants and Agreements, to implement Section 889 of the National Defense Authorization Act for 2019. The regulations prohibit the procurement and use of certain covered telecommunications equipment and services produced by the covered Chinese companies. The OMB’s proposed regulations would create 2 CFR 200.216, providing that “[g]rant, cooperative agreement, and loan recipients are prohibited from using government funds to enter into contracts (or extend or renew contracts) with entities that use covered technology.” According to the OMB, the prohibition “applies even if the contract is not intended to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services.” Comments were due on or before March 23, 2020.

The DoD held a [public meeting](#) on Part B on March 2, 2020. Several trade associations gave feedback, and raised five major concerns:

1. The broad scope of the rule;
2. The inability of many contractors to meet the August 2020 compliance deadline;
3. Whether the rule will apply outside the United States;
4. Whether the term “use” would include a reseller’s commercial sales of prohibited products, thus precluding a supplier from contracting with the federal government; and
5. Whether the “entity” subject to the ban includes only the legal entity executing the contract with the federal government, or also its affiliates and subsidiaries.

Unfortunately, DoD did not indicate when an interim rule might be issued. While commentators estimate that one or more interim rules on part B are expected out in mid-2020, the issuance of interim rule on part B is likely to be delayed by the COVID-19 pandemic. In fact, the industry has made repeated requests to extend the effective date for part B due to COVID-19. In addition, two U.S. senators, Marco Rubio (R-FL) and Ben Cardin (D-MD), have called on the OMB to ensure that federal regulation banning the government’s use of Chinese telecommunications technology include “explicit processes” to help small businesses with compliance, and

Sen. Rubio further urged the federal government to give small businesses more time to comply with a regulation restricting the use of certain Chinese telecommunication equipment. While it remains unclear when the interim rule might be released and whether an extension will be granted, companies are encouraged to closely monitor the Federal Register and provide comments when any proposed rules are published. Companies are further encouraged to reach out to their representatives or industries to seek an extension if they might be impacted by the implementing of part B, particularly given the disruptive impact of COVID-19.

What are "covered telecommunications equipment or services?"

Specifically, Section 889 creates a general prohibition on telecommunications or video surveillance equipment or services produced or provided by the following companies (and associated subsidiaries or affiliates):

- Huawei Technologies Company; or
- ZTE Corporation

It also prohibits equipment or services used specifically for national security purposes, such as public safety or security of government facilities, provided by the following companies (and associated subsidiaries or affiliates):

- Hytera Communications Corporation;
- Hangzhou Hikvision Digital Technology Company; or
- Dahua Technology Company

Notably, the definition under the NDAA and the initial interim rule includes "any subsidiary or affiliate" of the five Chinese entities named, without naming the entities' subsidiaries or affiliates, leaving the companies to identify who are subsidiaries or affiliated of the above identified entities. The second interim rule lessened companies' burden a bit, adding paragraph (d) to [FAR 4.2102](#), stating that the government will list the banned entities, "including known subsidiaries or affiliates," to the SAM's excluded parties list, via SAM.gov, "with an appropriate notation to identify that the prohibition is limited to certain products and services—the entity itself is not excluded." The representation at FAR 52.204-26 requires an offeror to review the list of excluded parties in SAM.gov and confirm whether the equipment or services it is providing the government come from one of these entities. The definition of "covered telecommunications equipment or services," to include any subsidiary or affiliate of the five Chinese entities named, however, remains unchanged.

While the prohibitions are initially limited to the five named companies, Section 889 authorizes the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the FBI, to extend these restrictions to additional companies based on their relationships to the Chinese government. This will, of course, require contractors to continuously monitor the Government's identification of new entities and

the impact that has on its supply chain.

Application

In summary, Section 889 includes three essential requirements:

1. Representation requirement under FAR 52.212-3 (Offeror Representations and Certifications-Commercial Items), FAR 52.204-24, (Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment) and 52.204-26 (Covered Telecommunications Equipment or Services-Representation);
2. Sale prohibition requirement under Section 889(a)(1)(A) of the NDAA and FAR 52.204-25 (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment) (part A); and
3. Use prohibition requirement under Section 889(a)(1)(B) of the NDAA and FAR 52.204-25 (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment) (part B).

Representation requirement

Section 889 mandates contractors to submit a representation with their offer identifying any “covered telecommunications equipment or services” that will be provided under the contract. The second interim rule permits an offeror to represent annually, via SAM.gov, whether it provides “covered telecommunications equipment or services as part of its offered products or services to the government in the performance of any contract, subcontract, or other contractual instrument,” instead of respond to every offer. [FAR 52.204-26](#).

If an offeror represents that it does not provide covered telecommunications equipment or services to the government in response to FAR 52.204-26 or [FAR 52.212-3\(v\)](#), then it is not required to complete the representations in FAR 52.204-24. However, it is very important that contractors to make the best effort to ensure the response is accurate.

However, if the offeror represents that it does provide covered telecommunications equipment or services, or has not made any representation in FAR 52.204-26 or FAR 52.212-3(v), it must still complete the representations required by FAR 52.204-24. Under FAR 52.204-24, if a contractor checks that it “will” provide covered telecommunications equipment or services, the contractor must identify all such equipment or services and describe its proposed use under the contract to enable the government to make a determination regarding whether use of the identified equipment or services rises to the level of a “substantial or essential component of any system” or “critical technology as part of a system.” “Substantial or essential component” means “any component necessary for the proper function or performance of a piece of equipment, system, or service.” Notably, the representation is NOT limited to

situations where the technology is “substantial or essential.” Instead, the representation captures any covered product or services and it is up to the Government to decide whether such incorporation is substantial or essential.

The second interim rule also sets forth procedures at FAR 4.2103 for contracting officers to follow. The procedures provide that a contracting officer “may rely” on a contractor’s representation in response to FAR 52.204-24, FAR 52.204-26 or FAR 52.212-3(v), “unless the contracting officer has a reason to question the representation.” Thus, while the definition of “covered telecommunications equipment or services” is not as definitive, it seems that an offeror’s review of the entities listed in SAM.gov (including all known subsidiaries or affiliates), and representation that it is not providing covered equipment or services from these entities, should be sufficient.

Section 889 further includes a continuing reporting requirement in the event the contractor discovers use of covered equipment or services during performance. Reports are to be made within one business day from the date of discovery. A follow-up report is required within 10 business days of the first report with additional information on the contractor’s mitigation actions.

Sale prohibition requirement

The sale prohibition requirement prohibits executive agencies from purchasing covered telecommunications equipment or services from certain Chinese telecommunications companies. Technically, while the regulation applies only if the covered equipment or services amount to “substantial or essential part,” such limitation is not particularly helpful in practice. As noted earlier, the representation is NOT limited to situations where the technology is “substantial or essential,” and instead captures all products or services incorporating covered products or services. The definition of “substantial or essential,” explained above, is quite broad and annoyingly circular, making it almost impossible to determine whether something is substantial or essential.

The sale prohibition requirement is to be flowed down in all subcontracts. In fact, the FAR Council has also updated FAR 52.244-6 and FAR 52.212-5(e), which includes the list of “mandatory” flow-downs for commercial item subcontracts. This means that prime contractors should be updating their subcontracts to include this latest flow-down requirement.

Use prohibition requirement

The use prohibition requirement contains a broad prohibition relating to the use of covered products and services incorporating certain Chinese technology, whether or not in the context of a federal contract. That is to say, the use prohibition includes no exception for internal uses unrelated to federal contracting. It contains no “nexus” requirement which would limit its application to uses “in connection with” a contract or subcontract. In other words, the prohibition is very far reaching and applies even if the

use of covered equipment or services is completely unrelated to federal business.

To date, the government has not given a list of products incorporating covered technology that need to be reported. What made it even more difficult for companies to comply with is the prohibition is not limited to end products produced by those Chinese entities; it covers most any product that incorporates technology provided by those Chinese entities. It could even apply to the foreign office of a U.S. entity with a government contract. It is possible that the interim rule on part B will include more guidance, but the government did not leave companies much time to build its compliance program.

At this point, it is unclear whether the use prohibition requirement will include any flow down requirements, but most of the commenters believe such requirement will still be included.

Without legislative changes, this requirement will likely go into effect in August 2020.

The exceptions

Section 889 contains two exceptions under which the above stated sale and use prohibitions do not apply:

1. It allows executive agencies to procure services that connect to the facilities of a third party, "such as backhaul, roaming, or interconnection arrangements." This likely means telecommunications providers are permitted to maintain common network arrangements with the covered entities.
2. It permits covered telecommunications equipment that are unable to "route or redirect user data traffic or permit visibility into any user data or packets" it might handle, meaning a contractor may still be able to provide services to the government so long as any covered equipment provided is unable to interact or access the data it handles.

Waivers

Section 889 allows for the head of any federal agency to issue a waiver of the prohibition for up to two years where the entity applying for the waiver provides a compelling justification for the additional time needed to implement the requirements and submits a "full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain," as well as the entity's plan to eliminate the prohibited equipment or services from its systems. The provision also allows the director of national intelligence to provide a waiver where he or she deems it to be in the national security interests of the U.S. However, it is expected that opportunities for waivers are very limited, justification for waivers require a high hurdle and such waivers will only be granted in the exceptional circumstances.

Practice Considerations – How to Ensure Compliance

As Section 889 part A already is in effect, and part B will likely goes into effect in August 2020, companies should carefully evaluate its global supply chain, the amount of federal government contract is currently has or will likely obtain, the possibility, cost and other impact to make necessary supply chain switches to eliminate the Covered Telecommunications Equipment or Services, and determine whether it the company would like to continue to contract with the federal government. Companies impacted should further consider to engage its own lobbyist, particularly given the interim rule has not been released.

To the extent that companies decides to continue to contract with the federal government, it is of crucial importance that they take immediate action to ensure compliance. While not comprehensive, below are some compliance considerations:

1. Determine whether the organization provides a product or service to the U.S. government, and/or performs under the terms of a grant for the U.S. government. In making this assessment, consider all possible federal agreements. For health care industries, for example, consider contracts with the VA, HHS, DHA, and OPM.
2. Develop an internal communications and plan to educate key stakeholders within the company on Section 889 and the company's prospective compliance obligations. Educate the organization's purchasing/procurement/materials management professionals to ensure they are up to speed on Section 889 requirements.
3. Identify potential covered products and technology in the company. The company's Chief Information Officer (or designee) should begin developing an inventory of technology that uses covered entity products or services. It should focus on products manufactured by Huawei and the four other Chinese entities and their affiliates and subsidiaries (many have been added to the Department of Commerce excluded entity list). Below is a list of products commonly manufactured by these companies:
 - Huawei: mobile phones, laptops, tablets, routers, and switches
 - ZTE Corporation: mobile phones, mobile hotspots, and network equipment, including routers and switches
 - Hytera Communications Corporation: radio transceivers and radio systems
 - Dahua Technology Company and Hangzhou Hikvision Digital Technology: video surveillance products and services (which may be part of a company's security system)

Companies should also consider any personal technology employees may use for work, such as phones, laptops, home routers, etc. The inventory should identify each item's function and location within the company.

Also consider whether any telecommunications technology from “approved” vendors may nevertheless contain Huawei or other banned components (e.g., camera system containing a Hytera circuit board).

Though the ban applies to equipment that is a “substantial,” “essential,” or “critical” part of a system, do not attempt to apply these terms in preparing the inventory (to avoid taking too narrow a view in the initial assessment).

4. Categorize direct and indirect purchases by risk. For example, the purchase of a hammer or a blue-tooth enabled hospital bed may be low risk; the purchase of a multifunction copier or thermostat may be medium risk; the purchase of a medical monitoring device with communications capabilities likely is high risk.
5. Develop a standard, written, risk-based process for evaluating the content of the various products. Perhaps the process calls for no diligence with respect to low risk items, obtaining a certification from sellers from which medium risk items are procured, and obtaining a certification coupled with additional due diligence for high-risk items. The process should be memorialized in writing, applied consistently, and monitored and audited periodically.
6. Engage your purchasing department to help determine the sources of the medium and high risk items. Prepare an inventory of indirect purchases similar to the process most of us already use for direct subcontract purchases.
7. Evaluate impact of Section 889 and compliance cost. Based on the foregoing review, evaluate compliance costs and possibility to find alternative suppliers. Although the interim rule has not yet been published, it is possible that, like part A, part B will implement a flow down clause or require certification language.
8. Solicit the necessary representation of compliance from the appropriate distributors or manufacturers, and ensure a process is in place to track the requests and the responses.
9. Monitor rulemaking. Consider whether the questions and costs presented warrant outreach during rulemaking to your government relations team, submitting comments on the interim rule, or coordinating with those industry organizations currently advocating on behalf of contractors on Section 889 rulemaking.
10. Track Costs. Compliance with part B will likely be very costly. Separately account for compliance costs, as they may be recoverable. Adopting a robust, risk-based compliance approach along these lines not only will help reduce the likelihood of noncompliance, it will help demonstrate a reasonable, good-faith effort to comply should compliance efforts turn out to be less than perfectly implemented.

What are the risks of noncompliance?

While compliance with such a far-reaching rule may seem costly, and it will be, not complying with the rule will be even more so. As a strictly contractual matter, an organization's failure to submit an accurate representation to the Government constitutes a breach of contract that can lead to cancellation, termination and a host of financial consequences. However, the primary fear will be the potential for an alleged False Claims Act violation based on noncompliance with Section 889. This liability can reach even those providers and subcontractors not directly covered by Section 889 if, by using the prohibited technology themselves, they cause prime contractors to submit false claims for payment to the government. Because the Government can seek treble damages and up to \$23,000 in penalties per a False Claims Act violation, the cost of merely defending against and resolving an allegation of a False Claims Act violation can be enormous. While the government may be inclined to give contractors, payers, and providers an adjustment period before opening intrusive audits and investigations, plaintiffs' lawyers will not be so generous.

For more information please contact [Yuanyou Yang](#) or any member of Porter Wright's [International Business & Trade Practice Group](#).