Government Contracts Cyber Café Series

troutman pepper

STRATEGIC CYBER PARTNERS

FAR and DFARS Provisions: Prohibited Telecommunications Equipment and Buy American

Straight Talk on Section 889 of the FY 2019 National Defense Authorization Act: Prohibition on Certain Telecommunications Services, Equipment, and Components

Follow-up to the September 15, 2020 webinar

Speakers

- **Hilary S. Cairnie**, Partner, Government Contracts practice, Troutman Pepper
- **Heather Engel**, Managing Partner, Strategic Cyber Partners, LLC

Welcome and Introduction

Disclaimer: In these sessions, we do not address the civilian agency counterpart regulations appearing at FAR Subpart 4.19.

Disclaimer: These sessions do not provide legal or technical advice specific to your organization, but only strive to heighten your awareness of the many moving parts associated with DOD's regulatory framework for cyber compliance.

Today's program — the Huawei ban — resulted from the numerous inquiries received by Heather and me in recent months as agencies have scrambled to impose the affirmative representation requirements (effective August 13, 2020) on contractors.

Reference Resources

- Section 889 of the FY 2019 National Defense Authorization Act
- FAR 4.2102, 2103, 2104
- FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
- FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
- FAR 52.204-26 Covered Telecommunications Equipment or Services-Representation

Quick Side Bar

Since our last program in June (we missed you!!!!), Troutman Sanders and Pepper Hamilton successfully merged on July 1, 2020. Troutman Pepper is a national law firm known for its higher commitment to client care. With more than 1,100 attorneys in 23 U.S. cities, the firm partners with clients across every industry sector to help them achieve their business goals.

Overview — the Huawei ban — What are we talking about?

While many people know the Huawei ban affects the worldwide build out of 5G networks, for the government contracting community, it means so much more.

The U.S. government has imposed a broad prohibition on the use of "covered telecommunications equipment or services" produced or provided by certain enterprises located in China and/or associated with the Chinese government.

This prohibition covers equipment from Huawei Technologies Company or ZTE Corporation, as well as video surveillance and telecommunications equipment or services produced and provided by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiaries or affiliates of the five entities (collectively, the "covered companies").

What constitutes telecommunications equipment and services?

Our understanding of telecommunications is that there are three basic elements — transmit, transport, and receive. Telecommunications can be wired or wireless. Devices include repeaters, hubs, switches, bridges, routers, gateways, voice over IP switches, mobile devices, facsimile machines, and even landlines.

Huawei was the largest telecommunications equipment vendor by revenue in 2017.

In formulating the operative regulations and clauses, the FAR council did not provide a definition for "telecommunications equipment" or "telecommunications services" — intentionally or unintentionally. No such guidance appears in the clauses at 52.204-24, 25, or 26. Therefore, we look elsewhere for definition.

Statutory Guidance: The Communications Act of 1934, 48 Stat. 1064, Ch. 652, June 19, 1934, as amended, created the Federal Communications Commission (FCC). See 47 U.S. Code § 153 – Definitions:

> *(50) The term "telecommunications" means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.*
>
> *(52) Telecommunications Equipment. Equipment other than customer premises equipment used by a carrier to provide telecommunications services.*
>
> *(53) The term "telecommunications service" means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.*

Regulatory Guidance: 48 CFR 239.7401 (NSA acquisition supplement) offers the following definition:

> *"Telecommunications" means the transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.*

Should contractors rely on the above definitions in conducting internal due diligence?

The better question is: Is it reasonable for contractors to rely on the above definition(s) in conducting internal due diligence?

That is a business judgement about which reasonable minds might differ.

Why are these companies' products banned?

Huawei reportedly has close ties to Chinese government officials, offices, and agencies and in the past, has shown a willingness to export technology to sanctioned countries, including North Korea and Iran.

There is potential for telecom equipment to be used for spying on populations around the world. Examples:

- Location data
- Traffic volumes and flows
- Backdoors built into equipment

In theory, controlling the tech at the heart of these networks could give Huawei or other companies the capacity to spy or disrupt communications during any future dispute. More things connected to networks — including over 5G, from self-driving cars and refrigerators to baby monitors and fire alarms — provide more avenues for disruption.

Attackers, state-sponsored and otherwise, could use these devices, which often have weak security features as back doors into strategically vital networks.

Parts A and B of section 889(a)(1) of the national defense authorization act of 2019 establish the Huawei ban.

The Part A prohibition became effective on August 13, 2019, and the Part B prohibition on August 13, 2020.

The Part A prohibition addresses what the government procures from the contractor, while the Part B prohibition focuses on what the contractor uses in its business.

Part A applies only to what you provide to the government under a contract and is a required flow-down.

The Part A prohibition (under FAR 52.204-24 and 204-25) requires contractors providing, i.e., delivering, "covered telecommunication equipment or services" to the federal government to:

> *…reconfigure their supply chains to exclude Huwaei/ZTE components (and the other covered telecommunications equipment) in the end products or services delivered to the government.*
>
> *Contractors are required to represent to the government annually whether the supplies or services they offer include covered telecommunications equipment or services.*
>
> *They are also required to report to the government when covered telecommunications equipment or services are used during contract performance.*
>
> *Part A prohibition is a required flow-down.*

Under Sec. 889(a)(1)(A), the federal government cannot "**procure or obtain** or extend or renew a contract to procure or obtain **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**."

So, already the lawyers are looking for potential loopholes:

If there is included covered telecommunications equipment (*i.e.*, Huawei or other), is that equipment "a substantial or essential component" of the system, or does it form a critical technology as part of such system?

See FAR 52.204-25 for definitions.

Part B applies to the prime contractor's use of covered telecommunications equipment and services - there is no distinction as to the nature of such use.

The Part B prohibition precludes the government from contracting with a company that "uses" any of the covered telecom services.

> *Currently, Part B applies only to the entity that contracts with the government, the prime contractor, and is not required to be flowed-down to subcontractors.*
>
> *For separation purposes, it will matter whether the prime contractor is a subsidiary or an operating segment (but not a separately formed company). If the contracting entity is not a separate subsidiary, the Part B prohibition will likely apply to the whole company.*
>
> *The government is considering expanding the rule to include affiliates, parents, and subsidiaries before finalizing the rule.*
>
> *Until such time as the final rule is issued, only the contracting entity and not its affiliate or parent companies are subject to Part B prohibition.*
>
> *The Part B prohibition encompasses the entity's use of covered telecommunications equipment and services:*
>
> > *not in connection with what it delivers to the government under a contract, and*
> >
> > *includes any such use for commercial or operational purposes.*
> >
> > *The Part B prohibition is not a required flow-down.*

The statutory language provides in relevant part that the federal government cannot **enter into** (*i.e.*, award) or extend or renew contracts with any **entity** that "**uses** any equipment, system, or service **that uses covered telecommunication equipment** or services **as a substantial or essential component of any system**, or as **critical technology as part of any system**."

USES. Notice that the word "uses" is reflected in both Parts A and B. The meaning of the word "uses" may prove to be pivotal to the administration and enforcement of these statutory prohibitions — but neither the statute nor the implementing regulations provide a definition for the term "uses."

Part B, using the term "entity," seemingly is limited to prime contract application, suggesting that it is not flowed-down to subcontractors.

The Part B prohibition may well have much broader impact on prime contractors. The statutory language arguably requires significant interpretation from regulatory authorities.

Arguably, under the Huawei ban, the government is prohibited from doing business with a contractor that has an internet service provider (ISP) that uses Huawei/ZTE equipment in providing internet service — whether that ISP supports a government contract or a commercial contract.

Or, contractor's use of covered telecommunication equipment (e.g., video surveillance cameras) for nonrevenue generating activities (e.g., building security) arguably could run afoul of the prohibition. As between the contractor and the agency, whose interpretation will be binding?

How do parts A and B potentially impact prime contractors and subcontractors?

We look to the contract clauses for insight.

Bear in mind, the clauses are interim, not final, and could change as a result of public comments.

Which contractors are covered by the FAR clauses?

Part A prohibition: All contractors and subcontractors.

Part B Prohibition: Prime contractors only.

FAR 52.204-24. This is a representation clause, which requires the contractor to affirmatively represent compliance or the extent of compliance.

Under Subparts (b)(1) and (2), the contractor represents whether it is or is not providing covered telecommunications equipment or services (Part A prohibition), and whether it does or does not use covered telecommunications equipment or services (Part B prohibition).

The (b)(1)and (b)(2) representations are not required if the contractor represents in response to 52.204-26, Covered Telecommunications Equipment or Services - Representation, that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the government in the performance of any contract, subcontract, or other contractual instrument."

For example, if the contractor is offering janitorial supplies, or hand tools, or mechanical fasteners and similar "non-IoT" tangible items, then the prohibition of Part A should not present any compliance problems. But, the contractor could still have compliance challenges under Part B if it uses covered telecommunications equipment in its operations.

FAR 52.204-25. Prohibition on contracting for certain telecommunications and video surveillance services or equipment. This contract clause includes important defined terms that apply to related clauses at 52.204-24 and 26.

(a) Key definitions: They are all key!!!

Critical technology means:

(1) Defense articles or defense services included on the U.S. Munitions List found in the International Traffic in Arms Regulations under subchapter M of Chapter I of Title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List in Supplement No. 1 to Part 774 of the Export Administration Regulations under Subchapter C of Chapter VII of Title 15, Code of Federal Regulations, and controlled.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Does your deliverable fit within the scope of defined loopholes?

In conducting contractor due diligence for compliance with Parts A and B prohibitions, the contractor must become well informed of these definitions. This clause also describes the scope of exceptions, the availability of the waiver process, and the obligation to self-report non-compliance.

The Part A prohibition appears under (b)(1), in part: "the Contractor is prohibited from providing to the Government 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, **unless** an **exception at paragraph (c) of this clause applies** or the covered telecommunication equipment or services are covered by **a waiver described in FAR 4.2104**."

The Part B prohibition appears under (b)(2), in part: No contracting "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, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract."

The exceptions at (c) concern (1) third-party interconnection arrangements, such as backhaul or roaming; and (2) telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

Finally, under Subpart (d), if at any time the contractor learns that it is not complying with the prohibitions, it must affirmatively disclose that fact and the associated details to the government: https://dibnet.dod.mil/.

This disclosure requirement feels an awful lot like the disclosure of 252.204-7012 to report cyber incidents.

FAR 52.204-26 Covered Telecommunications Equipment or Services-Representation.

The representation is as follows:

"(c) Representation. The Offeror represents that it □ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument."

The above representation pertains to the Part A prohibition. If the offeror offers not to provide covered telecommunications equipment or services to the government, then it need not submit the related representation of FAR 52.204-24.

However, if the offeror does offer to provide covered telecommunications equipment to the government, then it must also provide the related representation under FAR 52.204-24.

Finally, the Part A prohibition requires flow-down to subcontractors, while the Part B prohibition does not under FAR 52.204-25:

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2) [the Part B prohibition], in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

The Parts A and B prohibitions have caused contractor confusion in how they should represent to the government and their supply chain.

How will parts A and B impact subcontractors? What about the supply chain?

We know that Part A is a required flow-down because it pertains to what is ultimately delivered to the government.

Part B is not a required flow-down since the government lacks privity of contract with all subcontractors and therefore has no standing to enforce the Part B prohibition beyond the level of prime contractor. Practically speaking, what this means is that subcontractors should be able to use covered telecommunications services without restriction.

But, separate and apart from subcontractors (i.e., those entities that provide value added services or tangible items), what about prime contractor's other institutional service providers and equipment vendors? Internet service providers (ISPs), software as a service (SAAS) providers, surveillance and security equipment, routers, modems, IT system components, laptops, storage devices, mobile devices, etc. What if these items incorporate covered telecommunications equipment?

What level of corporate due diligence is required?

FAR 52.204-24: Representation. The offeror must represent to the government that your company will or will not provide covered telecom equipment or services, and **in order to provide an informed representation, you must conduct a reasonable inquiry of your company's devices to determine if the company uses covered telecom equipment.**

If you are a company with international offices, or for example you provide video surveillance to a base or government facility, you need to fully understand these rules and the applicability to your infrastructure and contracts you may have with the government. Not only that, you should understand how and what you are representing to the government.

Next steps?

The Federal Register notice (https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-15293.pdf) prescribes the following actions:

You must learn about the provision and the requirements.

You must inventory worldwide assets to identify covered telecommunications equipment and critical technology.

You will also need a compliance plan that includes (1) regulatory familiarization, (2) corporate enterprise tracking, (3) education, (4) cost of removal, (5) representation to the government, and (6) cost to develop a phase-out plan or submission of waiver information.

Also remember that Part B is still an interim requirement. Industry has until mid-October to submit feedback.

How do we answer the representation?

1. Our company works for the U.S. government as both a prime and sub with a robust commercial business. Our China offices use covered telecom equipment for backhaul. How do we represent today? How do we represent in the future?

   In this case, the contractor must look at several things. First, what services are being provided out of the China office? Are those services provided to the U.S. government? If so, then the representation answer is likely "yes" — covered telecom equipment is in use and you must represent, as well as develop a plan to act quickly and remove the covered equipment, or risk losing government contracts.

2. Our company delivers a medical device to our government end users; it includes a server with operating system and proprietary applications. It includes components and software that enables it to connect wirelessly to the internet and transmit/receive patient data using customer-provided facilities, equipment, and third-party internet service. Does my system constitute telecommunications equipment under the Part A prohibition?

   The company should inventory the system to determine first if the system contains any components from the banned companies. If not, then there is no applicability. If it does, then the system very well may constitute telecommunications equipment, and further due diligence is needed. The company should also consider what type of information is being processed, stored, or transmitted — a medical device may contain PII, PHI, or other forms of controlled unclassified information.

3. Our company performed rudimentary due diligence of our deliverable to the government, but did not have time to perform supply chain due diligence. Our representation was accepted by the contracting officer. Do I need to perform additional due diligence for Part A? For Part B?

   Yes, for both! You must be able to prove that you performed due diligence and acted in good faith.

4. We are a small business construction company operating under multiple NAICS codes. We construct turnkey buildings and perform renovations and improvements — all of which include primary trades, such as electrical, HVAC, plumbing, and security systems, all of which we subcontract to others. Am I even covered by Parts A and B prohibitions?

   Yes, any company performing work under a government contract is covered. In particular, engineering and construction firms must diligently manage their supply chain to ensure that covered equipment is not in use — video surveillance products and network infrastructure are two particularly common examples in this type of industry.

5. What if we just ignore the requirements at FAR 204-24, 25, and 26? What is the worst that can happen?

   This is an example of when ignorance is not bliss. Choosing not to be informed of applicable compliance obligations arguably could be viewed as a form of reckless disregard, a conscientious choice on the part of management. Reckless disregard can give rise to administrative, civil, and criminal proceedings and the need to incur significant legal cost to try and resolve such proceedings.

   Moreover, it is not likely that a contracting officer will fail to impose the certification requirements in covered solicitations, or that the presence or absence of such certifications will be overlooked during proposal evaluation. The point being, if you ignore the certification requirement, your offer will likely be rejected without evaluation. On the other hand, if you execute the certification without having performed reasonable due diligence, you risk submitting an erroneous certification, perhaps even a false certification, statement, and/or claim. 18 USC 1001.

   Bottom line: Do not throw the dice on the Huawei ban. Expend the due diligence, make informed judgments.

Program notes

As always, we welcome ideas for program topics, and will do our best to answer your questions. You may contact us at:

Hilary Cairnie - hilary.cairnie@troutman.com

Heather Engel - heather.engel@strategiccyberpartners.com