MEMORANDUM

TO: Clients Who Do Business with the Federal Government

FROM: LB3

DATE: April 16, 2020

RE: One More Thing to Worry About: Your Use of Banned Telecom Equipment

---

As if you don't already have enough on your mind, we are advising/reminding all clients who are federal government contractors that Congress has prohibited executive agencies from entering into, renewing, or extending contracts with entities that use certain foreign-made technology as of August 13 of this year, absent a waiver or an exception. The prohibition, which will be the second phase of a broader ban, applies to all federal executive agencies, including the Departments of Agriculture, Commerce, Defense, Energy, Education, Energy, HHS, Homeland Security, HUD, Interior, Justice, Labor, State Transportation, Treasury, and the VA.

Under the first phase of the ban, which took effect in August, 2019, government contractors must represent annually whether or not they provide any equipment, system, or service to the government that includes "covered telecommunications equipment or services" (described on Attachment 1) as a "substantial or essential component of any system or as critical technology as part of any system." If they do, they must describe how the covered equipment and services are used, including why their continued use is legally permissible or why a waiver of the ban would be justified.

In addition, if a government contractor discovers, while performing a contract, that it uses "covered telecommunications equipment or services" as a "substantial or essential component of any system or as critical technology as part of any system," or if it receives a similar notification from any of its subcontractors, it must report it to the government customer within one business day, including a description of how it is mitigating the impact of the banned technology.

Government contractors must "flow down" the substantive certification and reporting requirements described above to their subcontractors.

The second, more restrictive phase of the ban, which prohibits government contractors from even *using for any purpose* "covered telecommunications equipment and services" as a "substantial or essential component of any system or as critical technology as part of any system" (e.g., data processing in back office operations), has not yet been implemented through federal regulations, though an administrative

proceeding to adopt new rules is anticipated soon. We can only speculate whether the new rules will mirror the certification, reporting, and flow-down requirements that were adopted to implement the first phase of the ban, but we will monitor the progress of the new rules and follow up if/when they are announced.

In the meantime, companies that may buy telecommunications equipment and services from Huawei, ZTE Corporation, or any of their affiliates should consider conducting an internal audit to determine whether they use any that are, or contain, "covered telecommunications equipment or services," as described on Attachment 1, as a "substantial or essential component of any system or as critical technology as part of any system." Those that do should catalog each of the banned products and services, including a description of how they use each item on the list. The inventory should be kept up-to-date, as the company will likely need to consult it from time to time when participating in a federal government solicitation and (if required to do so) when making its semi-annual certifications.

It would also be wise for companies that use such technologies to keep records of the steps they are taking to identify and catalog any "covered telecommunications products or services" or products with banned components. These steps should include periodic (perhaps quarterly) inventory updates, maintaining copies of contracts the company has with subcontractors, showing that it has flowed down its obligations concerning banned technology to them, and copies of any correspondence with subcontractors regarding these obligations.

Please contact the LB3 attorney(s) with whom you work if you have any further questions.

Attachment 1

What are "covered telecommunications equipment and services" and when are they considered to be a "substantial or essential component of any system or … critical technology as part of any system."

"Covered telecommunications equipment or services" are defined in the National Defense Authorization Act for 2019 ("NDAA") and its implementing regulations. Essentially, they include:

- Telecommunications equipment manufactured by Huawei or ZTE Corporation;

- Certain video surveillance equipment manufactured by Hystera Communications, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company;

- Telecommunications or video surveillance services provided by any of the above companies; and

- Telecommunications or video surveillance equipment manufactured or sold by any entity that the Department of Defense, the Director of National Intelligence, or FBI Director determines to be owned and controlled by, or otherwise connected to, the government of the People's Republic of China.

Affiliates of the listed Chinese companies are included in the ban – a total of over 110 entities.

"Covered" equipment or services become problematic under the Act only if they are a "substantial or essential component of any system, or … critical technology as part of any system." Although the NDAA does not define these terms, the implementing regulations provide some guidance.

A "substantial or essential component" is one that is "necessary for the proper function or performance of a piece of equipment, system, or service," and may not contain or use "covered telecommunications equipment or services."

"Critical technology" includes virtually any product, service, or intellectual property (such as software) that is used for national defense (e.g., weapons, including biological weapons), nuclear power (including nuclear facilities and material), surreptitious intelligence gathering, and "emerging and foundational technologies" critical to our national security and whose export is banned by federal law.