

COMPLIANCE ALERT

AUGUST 2020

FEDERAL ACQUISITION REGULATION: PROHIBITION ON FEDERAL AGENCIES CONTRACTING WITH ENTITIES USING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

The purpose of this compliance alert is to raise awareness of the requirements and effective date (August 13, 2020) of the FAR clause and OMB Final Guidance implementing Section 889(A)(1)(B) of the National Defense Authorization Act (NDAA) for Fiscal Year 2019.

BACKGROUND

On July 14, 2020, the Federal Acquisition Regulatory Council issued an interim final rule implementing Section 889(a)(1)(B) of the National Defense Authorization Act (NDAA) for fiscal year 2019 (FY2019). Additionally, the Office of Management Budget (OMB) issued its Final Guidance¹ on implementation of Section 889.

FEDERAL ACQUISITION REGULATION

The new interim final rule, Part B, is part of a two-stage implementation of NDAA 2019's Section 889 restrictions on covered telecommunications equipment and services in government contracting.²

Effective August 13, 2020, the Part B interim final rule prohibits [federal executive agencies](#)³ from contracting, extending, or renewing a contract with an entity that:

- uses “covered telecommunications equipment or services” as a “substantial or essential component”⁴ of any system, or
- uses “covered telecommunications equipment or services” as “critical technology” (see below) as part of any system,

¹ <https://www.federalregister.gov/documents/2020/08/13/2020-17468/guidance-for-grants-and-agreements>

² <https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain>

³ <https://www.loc.gov/rr/news/fedgov.html>

⁴ Defined as “any component necessary for the proper function or performance of a piece of equipment, system, or service.”

This applies regardless of whether there is a nexus between such use and the contractor's performance of government contracts, unless an exception applies, or a waiver is granted.

The restrictions cover broad categories of telecommunications and video surveillance equipment and services produced and provided by: (1) Huawei Technologies Company Ltd., (2) ZTE Corporation, (3) Hytera Communications Corporation, (4) Dahua Technology Company Ltd., and (5) Hangzhou Hikvision Digital Technology Company Ltd., and their subsidiaries or affiliates.

CRITICAL TECHNOLOGY

The Interim Rule specifies that it does not change the definition that was adopted in the first interim rule of "critical technology," which was included in the Foreign Investment Risk Review Modernization Act Of 2018 (Section 1703 of Title XVII of the NDAA for FY 2019, [Pub. L. 115-232, 50 U.S.C. 4565\(a\)\(6\)\(A\)](#)).

"The term "critical technologies" means the following:

- (i) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations.
- (ii) Items included on the Commerce Control List set forth 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—
 - (I) pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
 - (II) for reasons relating to regional stability or surreptitious listening.
- (iii) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities).
- (iv) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material).
- (v) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code.
- (vi) Emerging and foundational technologies controlled pursuant to section 4817 of this title."

CERTIFICATION

The rule requires federal agencies to require all offerors to represent, after conducting a “reasonable inquiry,” whether covered telecommunications equipment or services are used by the offeror as a substantial or essential component or critical technology of any system. Currently, federal agencies require offerors to make compliance representations in each solicitation, proposal or contract ([FAR 52.204-24](#), “Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment” and FAR 52.204-25, “Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment”). The FAR Council intends to issue subsequent rulemaking that will allow a contractor to represent in the System for Award Management (SAM) that it “does” or “does not” use the banned technologies, after making a “reasonable inquiry.”

ACTION REQUIRED: REASONABLE INQUIRY

In order to certify compliance, the rule indicates contractors must make “an inquiry designed to uncover any information in the entity’s possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity.” This includes examining relationships with any subcontractors or suppliers for which the prime contractor has a Federal contract and uses the supplier or subcontractor’s “covered telecommunications” equipment or services as a substantial or essential component of any system. The rule does state that this “reasonable inquiry” assessment does not require a contractor to complete an internal or third-party audit.

COMPLIANCE PLAN REQUIRED

FAR Council recommends that contractors develop and implement compliance plans, which should include at least the following:

- An understanding of the Section 889 requirements;
- A system for determining through a reasonable inquiry whether any covered equipment or services are used as a substantial or essential component of any system, or as critical technology as part of any system. This should include consideration of shared technology and services as well as an examination of subcontractor and supplier relationships – this will likely need to occur when a supplier or subcontractor is first used, when significant changes occur within the entity, and annually after the initial inquiry;
- training of sourcing personnel (e.g., purchasing/procurement and materials management) to ensure their awareness of the Section 889 prohibitions and requirements as well as the requirements of the compliance plan;
- procedures for replacing any covered telecommunications equipment or services once identified;
- a plan for updating previously provided representations, and for providing notification to the Contracting Officer (CO) if any covered telecommunications equipment or services are identified; and
- a plan for requesting any necessary waivers.

OFFICE OF MANAGEMENT BUDGET FINAL GUIDANCE

In addition to the Federal Acquisition Regulation requirements referenced above, on August 13, 2020, the Office of Management Budget (OMB) issued its Final Guidance⁵ on implementation of Section 889. The amendment to 2 CFR 200.216, prohibits grant and loan recipients and subrecipients from using federal funds to enter into, or renew, contracts for equipment, services, or systems that use covered telecommunications equipment or services as a substantial or essential component of any system or critical technology as part of any system.

§ 200.216 Prohibition on certain telecommunications and video surveillance services or equipment.

(a) Recipients and subrecipients are prohibited from obligating or expending loan or grant funds to:

- (1) Procure or obtain;
- (2) Extend or renew a contract to procure or obtain; or
- (3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems 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. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(ii) Telecommunications or video surveillance services provided by such entities or using such equipment.

(iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

See the Federal Register document for the full text of OMB's revised [Guidance for Grants and Agreements](#).

ECAS Research Compliance developed this compliance alert in partnership with the following University of California Systemwide Offices: Research Policy Analysis & Coordination, the Office of General Counsel, and Information Technology Services.

⁵ <https://www.federalregister.gov/documents/2020/08/13/2020-17468/guidance-for-grants-and-agreements>