

August 18, 2020

To: Contract & Grant Officers
Research Compliance Officers

Subject: Implementation of Section 889 of the National Defense Authorization Act (NDAA) for Fiscal Year 2019

Purpose

This memo provides guidance regarding the federal government's implementation of Section 889 of the National Defense Authorization Act (NDAA) for fiscal year 2019 (FY2019).

Background

The US federal government has issued rules and guidance that implement Section 889 of the National Defense Authorization Act (NDAA) for fiscal year 2019 (FY2019). This memo provides guidance for both contracts containing the Federal Acquisition Regulation (FAR) implementing clauses and for federal assistance awards (grants and cooperative agreements).

Federal Contracts

On July 14, 2020, the Federal Acquisition Regulatory Council issued an interim final rule implementing Section 889(a)(1)(B) of the NDAA for FY2019. 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 (See the attached ECAS Compliance Alert.)

Whereas prior prohibitions focused on covered defense telecommunications equipment or services products or services offered or provided to the federal government in the performance of any contract, subcontract, or other contractual instrument¹, the Part B implementation of the Section 889 codified in FAR clauses [52.204-24](#) and [52.204-25](#) has a much broader reach. It prohibits the federal government from contracting with an entity that simply *uses* "covered telecommunications equipment or services" as a substantial or essential component of *any* system, or "covered telecommunications equipment or services" as "critical technology" as part of *any* system. This prohibition applies whether or not such equipment or services are used in the performance of a government contract or part of contractual deliverables provided to the

¹ See [FAR 52.204-26](#) and [DFAR 252.204-7016](#)

government.

The government stated its rationale for the restriction in the publication of the Interim Rule. The government seeks to avoid disruption of federal contractor systems, which could in turn, disrupt the operations of the federal government, as it relies on contractors to provide a range of support and services. The government seeks to avoid exfiltration of sensitive data from contractor systems arising from contractors' use of covered telecommunications equipment or services as a substantial or essential component or critical technology of any system. Such covered telecommunications equipment or services are thought to present privacy and security risks.

FAR 52.204-25 has an effective day of August 13, 2020. Campuses may start seeing the clause in Department of Defense contracts, though recently there are unofficial indications of a delay. Campuses receiving federal contracts incorporating FAR 52.204-25 must develop and implement training and education, administrative controls covering purchases and technology, and mechanisms for removal for prohibited technology and for reporting of any identified prohibited telecommunications equipment or services as required by the clause.

Campuses with extramural federal contracts incorporating the clause must not use any equipment made 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 in University systems or research. This includes the use of personal phones/devices that connect with UC systems, including for multi-factor authentication purposes (e.g., DUO). Researchers should work with the campus ISOs or IT offices to find alternate technologies or devices (e.g., UC provided dongles).

Campus Sponsored Projects Offices, Research Compliance Offices, Procurement Offices and Information Security Offices (ISO) should coordinate to ensure compliance and broad awareness of the prohibition. Compliance plans should include at least the following action plans:

- All persons with procurement authorization (including low-level purchases) should be notified of the prohibition in order to minimize or eliminate the purchase of prohibited equipment or services;
- Researchers with federal awards should be notified of the prohibition so that they do not procure, use or attach prohibited equipment/technologies to University systems; and
- ISOs, Central IT and/or all Unit IT should conduct regular reasonable inquiries to identify suspect devices and remove network access as necessary.

See the attached Section 889 flyer issued by the federal government.

Federal Assistance Awards

In addition, on August 13, 2020, the Office of Management Budget (OMB) issued its [Final Guidance](#) on the implementation of Section 889. The amendment to Uniform Guidance 2 CFR 200.216 prohibits using federal funds to enter into, or renew, contracts for equipment, services,

or systems that use covered telecommunications as a substantial or essential component of any system, or as critical technology as part of any system.

The covered telecommunications equipment or services includes equipment produced by Huawei Technologies Company or ZTE Corporation and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company. It also includes equipment or services produced by any subsidiary or affiliate of such entities. The Secretary of Defense may also add entities it reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Campuses must inform researchers and those with purchasing authority (regardless of the dollar level) about this restriction on the use of grant/loan funds to purchase equipment or services produced by the entities listed above.

Subcontractor/Vendor Contracts or Subawards

Under both contracts and assistance awards, UC purchasing authorities and campus contracts/grants officers must flow down the requirements of FAR clauses 52.204-24 and 52.204-25, and 2 CFR 200.216, as applicable, in procurement contracts, subcontracts and subawards under federal contracts or grants.

Contact

Lourdes DeMattos
Research Policy Analysis & Coordination
Lourdes.DeMattos@ucop.edu
(510) 987-9850



Lourdes DeMattos
Associate Director
Research Policy Analysis & Coordination

Attachments: ECAS Compliance Alert
Section 889 flyer

cc: Information Security Officers
Material/Procurement Managers

SECTION 889

Section 889 ("Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment") is part of the Fiscal Year 2019 National Defense Authorization Act (NDAA). There are two prohibitions in the legislation, Part A and Part B.

RECOMMENDED CONTRACTOR COMPLIANCE ACTIONS

1. **Regulatory Familiarization.** Read and understand the rule and necessary actions for compliance.
2. **Corporate Enterprise Tracking.** Determine through reasonable inquiry whether you use "covered telecommunications" equipment or services.
3. **Education.** Educate your purchasing/procurement, and materials management professionals to ensure they are familiar with the entity's compliance plan.
4. **Cost of Removal.** Implement procedures if the entity decides to replace existing covered telecommunications equipment or services and ensure new equipment and services acquired for use by the entity are compliant.
5. **Representation.** Provide representation re use and alert Government if use is discovered during contract performance.
6. **Phase-out Plan and Submit Waiver Information.** Develop a phase-out plan and provide waiver information to the Government along with the complete laydown of the presence of the covered telecommunications equipment or services.

For more details see the FAR representation ([52.204-24](#), [52.204-26](#)) and FAR reporting ([52.204-25](#)) requirements.

For Details on the Recommended Compliance Steps: See the [FEDERAL REGISTER](#)

WAIVER PROCESS

Each agency must designate a senior agency official for Supply Chain Risk Management and participate in the Federal Acquisition Security Council's (FASC) information-sharing environment. Each waiver must include:

- A compelling justification for additional time needed
- A full and complete laydown of covered telecom
- A phase-out plan to eliminate the covered telecom

Agencies must consult with Office of the Director of National Intelligence (ODNI) and confirm that ODNI does not have information suggesting the waiver would present a material increase in risk to U.S. national security.

Agencies must also give a 15-day advance notification of waiver to the FASC and ODNI.

Agencies must notify Congress within 30 days of issuance of a waiver and must include:

- Requesting agency's attestation that granting waiver will not present a material increase in risk to U.S. national security
- Full and complete laydown of covered telecom equipment in the waived entity's supply chain, including a description of each category of technology equipment or service
- Required phase-out plan

TO SUBMIT COMMENTS TO THE FAR RULE

1. Go to <https://www.regulations.gov/>
2. Search for "FAR Case 2019-009"
3. Select corresponding "Comment Now" link and follow instructions

Why are these changes important?



The danger our Nation faces from foreign intelligence actors looking to infiltrate our systems has never been greater.

NDAA prohibitions against nefarious networks like Huawei will ensure our Nation remains secure. This



Administration is committed to working with Congress to keep America strong through implementing the NDAA prohibitions.

Bad actors are persistent in trying to infiltrate US networks – often exploiting technologies from the identified Chinese companies to do so. The Trump Administration shares Congress's strong commitment to addressing insidious threats to the Nation's national security and intellectual property.



The Federal Government alone experiences hundreds of thousands of digital assaults every day. Malicious actors are persistent, usually well-funded and constantly changing their tactics. They often exploit technologies from the identified Chinese companies to do so. The Administration shares Congress' strong commitment to addressing insidious threats to the Nation's national security and intellectual property.



The Trump Administration is keeping our government systems strong against nefarious networks like Huawei by leaning into Congress's Huawei ban with an aggressive posture.



Part A - The Government Cannot Obtain Prohibited Telecom

Part A became effective on **August 13, 2019**.

Part A prohibits the government from **obtaining** (through a contract or other instrument) certain telecommunications equipment (including video surveillance equipment) or services produced by the following *covered entities* and their subsidiaries and affiliates:

- **Huawei Technologies Company**
- **ZTE Corporation**
- **Hytera Communications Corporation**
- **Hangzhou Hikvision Digital Technology Company**
- **Dahua Technology Company**

The Department of Defense has the authority to add additional companies to this list.

Part A has been added to the Federal Acquisition Regulation (FAR) at [FAR subpart 4.21](#).

Note that the Part A ban also applies to **commercial items** ([FAR 12.301\(d\)\(6\)](#)) and **micro-purchases** ([FAR 13.201\(j\)](#)).

Have questions about GSA's implementation of Section 889? See [GSA's 889 Part A Q&As](#)

Part B - Government Contractors Cannot Use Prohibited Telecom

Part B is effective **August 13, 2020**.

Part B prohibits the government from contracting with any entity that **uses** certain telecommunications equipment or services produced by the *entities* listed in the statute.

- The Government cannot contract with an entity 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.
- Prohibition applies regardless of **whether or not** that usage is in performance of work under a Federal contract.
- The prohibition applies to **every sector** and **every dollar amount**. **Your ability to enter into contracts with the Government will be impacted by Part B.**
- After conducting a **reasonable inquiry**, entities will represent whether they **do or do not use** prohibited telecommunications equipment or services.

Part B has been added to the Federal Acquisition Regulation (FAR) at [FAR subpart 4.21](#).

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>