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.

China is increasingly asserting itself by stealing U.S. technology and intellectual property to erode U.S. economic and military superiority.

Chinese companies, including the companies identified in the FAR rule, are legally required to cooperate with their intelligence services. China's reputation for close collaboration between its government and industry to amass technological secrets presents additional threats to U.S. Government contractors.

The FAR rule ensures contractors keep national security interests in mind by ensuring that they do not use certain equipment and services that present national security concerns.

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 an 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.
- 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.