Office of Government-wide Policy

FY19 NDAA Section 889 Prohibitions

November 6, 2019

Section 889's Two Prohibitions

- Section 889 of the FY 2019 National Defense Authorization Act (NDAA) included two prohibitions for certain information and communications technology (ICT) products and services from Chinese entities:
  - Effective August 13, 2019, the Government is prohibited from procuring, obtaining, or extending or renewing a contract to procure or obtain, covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system
  - Effective August 13, 2020, the Government is prohibited from entering into a contract, or extending or renewing a 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

ICT Supply Chain Threat

- Cyber threats from foreign adversaries, hackers, and criminals present significant and new risks to government and industry[1]
- Foreign adversaries are increasingly creating and exploiting vulnerabilities in ICT in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the U.S.[2]
- Constant, targeted, and well-funded attacks by malicious actors threaten government and industry by way of their contractors, sub-contractors, and suppliers at all tiers of supply chain[1]

[1] DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force Webpage

[2] Executive Order on Securing the Information and Communications Technology and Services Supply Chain

ICT Supply Chain Threat, cont'd

- Sophisticated threat actors exploit vulnerabilities deep in ICT supply chain as beachhead from which they can gain access to sensitive information further along the supply chain[3]
- China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or disrupt critical infrastructure[4]
- China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems[4]

[3] Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force Webpage

[4] 2019 Worldwide Threat Assessment of the Intelligence Community

ICT Supply Chain Threat, cont'd

- China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies[4]
- China is improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens[4]
- The Government of China will authorize cyber espionage against key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means[4]
- There is concern about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies[4]

[4] 2019 Worldwide Threat Assessment of the Intelligence Community

Covered Telecommunications

- “Covered telecommunications equipment and services”[5]:
  - Telecommunications equipment produced and services provided by Huawei or ZTE;
  - Video surveillance and telecommunications equipment produced and services provided by Hytera, Hikvision, and Dahua;
  - Telecommunications or video surveillance services provided by such entities or using such equipment; or
  - Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, China

[5] Summary of definition within FAR 4.2101

Covered Telecom, cont'd

- Per FAR 4.2101, "substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service
- "Critical technology" is also defined at FAR 4.2101
- "Covered telecommunications equipment and services" does *not* include:
  - A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
  - Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data

FAR Subpart 4.21

- Implemented through FAR Case 2018-17 in response to Section 889
- Added the first prohibition from Section 889 to FAR 4.2102
  - The prohibition also applies to commercial items (FAR 12.301(d)(6))
  - The prohibition also applies to micro-purchases (FAR 13.201(j))
- Created a representation provision (FAR 52.204-24) for all new solicitations and a reporting clause (FAR 52.204-25) for all new and existing contracts
- The reporting clause requires contractors (flows down to all subcontractors) to notify the Government if covered telecommunications equipment or services are used during contract performance

GSA Deviation to Section 889

- GSA has developed a class deviation to limit the representation requirements to the IDIQ contract level instead of at the order-level for low and medium risk indefinite delivery contract vehicles
- Per the deviation, GSA requires representation and reporting clauses in all new solicitations
- The deviation also establishes implementation targets for modification of existing contracts to include both the representation and reporting clauses
- Because Section 889 applies to all contracts, including purchase card transactions and other award types, not just FAR-based contracts, GSA's deviation also applies this policy to GSA's lease acquisitions

Future FAR Actions - 1st Prohibition

- DoD, GSA, and NASA are currently working on 2nd interim rule to allow offerors to represent annually whether they sell equipment, systems, or services that include covered telecommunications equipment or services
- Only offerors that provide an affirmative response to the annual representation would be required to provide the offer-by-offer representation in their offers for contracts and for task or delivery orders under indefinite delivery contracts[6]
- The comment period closed for the 1st interim rule

[6] 84 FR 40216, published on 08/13/2019

Future FAR Actions - 2nd Prohibition

- A proposed rule to implement Section 889's 2nd prohibition is anticipated by January 2020
  - Effective August 13, 2020, the Government is prohibited from entering into a contract, or extending or renewing a contract, **with an entity that uses** certain covered telecommunications equipment or services
- When considering this 2nd prohibition, think about every tier of supply chain you have and about use unrelated to performance of a GSA contract
- There will be an opportunity to comment on the Federal Register website on both the 2nd interim rule for the 1st prohibition and the proposed rule for 2nd prohibition

Section 889 - 2nd Prohibition

Effective August 13, 2020,

the Government is prohibited from

entering into a contract,

or extending or renewing a contract,

with an entity that uses certain covered

telecommunications equipment or services

Closing

- Send additional comments and feedback no later than next Wednesday, November 13, 2019 to the GSA Procurement Ombudsman Office at: gsaombudsman@gsa.gov

- The Presentation slides will be available until close of business next Wednesday, November 13, 2019 at: https://interact.gsa.gov/GSA889IndustryEngagement