Title:
Section 889 Ban on Select China-Based Products: Solutions for Overcoming Regulatory Disruption

Authored By Baker Tilly: Jeff Clayton, Principal and Leo Alvarez, CFCM, Senior Manager

Snapshot

In the face of rising uncertainty over data security and surveillance by foreign adversaries, DOD, GSA, and NASA (collectively, the FAR Council) released an interim final rule last month banning Federal agencies from purchasing telecommunications and video surveillance equipment or services from certain Chinese entities.

The rule implements Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019. Designed to counter cybersecurity threats to the U.S. Federal Government's supply chain, federal agencies are prohibited from using or purchasing select items from five Chinese tech giants:

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- Certain public safety or surveillance applications produced by Hytera Communications Corporation, Dahua Technology Company, or Hangzhou Hikvision Digital Technology Company (or any subsidiary or affiliate of such entities);

The prohibition covers items that are "a **substantial or essential** component of any system, or as **critical technology** as part of any system" (more on this below).

Additionally, the rule requires companies to provide a disclosure of the presence of the banned items in their supply chain (including subcontractors / suppliers at any tier), applies below **and** above the simplified acquisition threshold, and also applies to purchases of commercial off-the-shelf items (COTs). The ban casts a wide net.

Effective August 13, 2019, Contracting Officers have already begun including two new FAR provisions in new contract solicitations (and solicitations slated for award on or after August 13th) to implement the prohibitions:

- 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.

Of particular note, the prohibition will extend to contractors themselves in **August 2020**. This means that the Federal government will be prohibited from contracting with organizations that use these banned items or services as a substantial or essential component of any system, or as critical technology as part of any system.

Given the prevalence of sourced components and technologies from companies concentrated in China, federal contractors (particularly in the information technology and telecommunications space) would be wise to carefully consider vendor management practices and exposure of their supply chains to these prohibited sources.

Potential Areas of Difficulty

- Vendor Management and Ubiquity of Prohibited Items
  How federal contractors respond to the regulation is made difficult by the ubiquity of the prohibited items. Huawei has previously been ranked as the world's top telecommunications supplier[1] and number two phone manufacturer[2]. One news outlet recently conducted a review for

[1] https://www.delloro.com/telecom-equipment-market-2018-2/
[2] https://www.idc.com/promo/smartphone-market-share/vendor

Hikvision and Dahua devices across the U.S. and found at least 200,000 devices in use[3]. Even organizations with tight control and visibility into their suppliers may find difficulty gaining a strong sense of whether prohibited items are in use if they are purchasing items where a prohibited source is an Original Equipment Manufacturer (OEM)[4] or if an item has been "white labeled" and repackaged under a different brand.

Subcontracting also presents its own vendor management challenges. As presently constituted, the rule requires federal contractors to monitor their subcontractors at all tiers. FAR 52.204-25 and FAR 52.204-24 contain mandatory flow down requirements to first-tier and lower-tier subcontractors, meaning that subcontractors are also prohibited from using the banned telecommunications technology or services. One can imagine the difficulties inherent in the common industry practice of partnering with "blank" as-a-service enterprises who maintain and manage their own information technology assets in servicing commercial customers, or in managing and understanding the existence of the banned items and services in a supply chain that may be multi-layered, complex and global.

- Assessing the Criticality of Equipment and Components
  The rule defines "substantial or essential" as "any component 'necessary' for the proper function or performance for a piece of equipment, system, or service." Absent adjudication or a specific ruling on the matter, only time will tell how this definition will be applied. Given the U.S. security posture, however, it would be wise to consider applying the definition broadly. The rule does specify two exceptions:

  (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

  (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

  This means that this kind of equipment could be used as long as the system does not have visibility into the data being processed through it.

  The interim rule adopts the definition of "critical technologies" from the Foreign Investment Risk Review Modernization Act (FIRRMA) – which, again, is meant to be far reaching. The definition includes technologies included on the United States Munitions List (USML) set forth in the International Traffic in Arms Regulations (ITAR), Commerce Control list set forth in Supplement No. 1 to part 774 of the Export Administration Regulations (EAR), and even emerging and foundational technologies controlled pursuant to Section 1758 of the Export Control Reform Act of 2018.

- Disclosure / Reporting Obligations
  As required in FAR 52.204-24, federal contractors must represent whether they will be providing covered telecommunications equipment or services to the government during contract performance. If so, the organization must provide a disclosure outlining:

  (1) All covered telecommunications equipment and services offered or provided (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

[3] https://www.forbes.com/sites/thomasbrewster/2019/08/21/2000-banned-chinese-surveillance-cameras-keep-watch-over-us-government-sites/#10b05e907f65

[4] In this context, an OEM is defined as an organization that produces equipment or components that are ultimately marketed by another manufacturer (selling the finished item to end users). In some cases/markets, this term may refer to the organization itself that is incorporating the components from other manufacturers into a single end product.

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

Moreover, if during contract performance a contractor becomes aware that it or one of its subcontractors/suppliers is using covered equipment, it has a single business day from the date of discovery to notify the government. The rule requires contractors to further describe the effort being made to mitigate the situation and to prevent future use of such telecommunications technologies or services within ten business days.

For many, the speed with which contractors are required to react, notify, and enact remedial activities to replace prohibited items could have wider repercussions for service delivery and overall business continuity. This is especially true for small business organizations with more limited resources for support. As such, it is incumbent on contractors to take action now if they suspect issues with their supply chain.

- Open Questions
  As an interim rule, the federal government has given industry 60 days to provide comment. If the FAR council is persuaded by any of the comments, they may amend the rule. However, given China's strong foothold in the telecommunications industry and the U.S. security posture, the basic purpose and prohibitions put forth by the rule are expected to remain intact. Contractors should expect a final rule before the end of the year.

Next Steps: What Should Contractors be Considering

- Supplier Expenditure / Data Review
  Federal contractors investigating the presence of covered telecommunications and surveillance equipment in their own supply chain may find comfort in examining supplier expenditures over a specified period of time (for example, a 12 to 24 month period) to uncover specific banned equipment or sources that are considered to be higher risk (distributors or resellers with ties to the specified banned Chinese entities). Shipping records can also be helpful in identifying OEM relationships where they are not apparent, and inventory records can help isolate higher risk equipment. Additionally, some MAC Address and OUI lookup applications[5] can be used to identify the manufacturer associated with certain kinds of equipment (for example, IP cameras). If these data points are inconclusive, interior labeling on equipment can also be used to draw alignment with banned sources.

- Vendor Agreement Review
  Given the risk to prime contractors from the blanket representation made in FAR 52.204-24, prime contractors may want to consider flowing down the representation to their subcontractors and suppliers to add a layer of assurance. Building 'right to audit' considerations into the contracting process and requiring the suppliers behave similarly may also be worthy of consideration. The rule flows down to all tiers, and suppliers should be encouraged to be active

[5] Organizational Unique Identifier (OUI), is the first 24 bits of a MAC address for a network-connected device, which indicate the specific vendor for that device. The Institute of Electrical and Electronics Engineers (IEEE) assigns OUIs to vendors.

participants in securing the supply chain. Mandatory monitoring activities and reporting to the prime may also be helpful in supporting the prime contractor's responsibilities in this area.

- Supply Chain Remediation and Transition Plan
  Given the reporting responsibilities, prime contractors should be ready to enact remedial activities to transition from one vendor to another should it be discovered that it is purchasing product or services from a banned source. In some cases this may mean supporting a subcontractor or supplier while it works to identify a different vendor. However, organizations would be wise to think about modeling the impact to service delivery (delays and shortages) and potential impacts to cost, while outlining a tactical plan for handling transitions (linkages to logistics and communications systems, transfer of information, and training), should a new supplier or subcontractor need to be identified and integrated quickly. Transition to an in-house service may also be an area that is considered.

- Policy and Procedure Updates
  Given that FAR 52.204-24 and FAR 52.204-25 will be present in all new and existing solicitations, contractors should be enhancing internal policy and procedure documentation to recognize the additional approver and designee responsibilities for activities associated with overseeing activities in this area. In some cases this may mean developing process flows and narratives for key corporate controls.

- Tracking Compliance Cost
  Contractors should carefully track the compliance costs to adhere to these new requirements as they may be reimbursable on fixed-price and cost-reimbursement contracts.

- GSA Class Deviation
  GSA recently issued a class deviation that simplifies the reporting requirements for certain GSA contracts deemed to be low or medium risk. High risk contract vehicles will require a supply chain representation at both the contract and order level. Low and medium risk contracts will only have to provide a representation at the contract level. A list of high-risk GSA Schedule contracts include:
  - **Telecommunications Contracts:**
    - Networx,
    - Enterprise Infrastructure Solutions (EIS),
    - Connections II, and
    - Local Telecommunications
  - **Federal Supply Schedules Contracts**:
    - 36, 58 I, 70, and 84 (or the equivalent SINs under the MAS Reform Structure)
  - **IT Governmentwide Acquisition Contracts (GWACs)**
    - Alliant 2,
    - Alliant 2 SB,
    - VETS 2, and
    - 8{a) STARS Ill
  - **Commercial Solution Opening Procurements (CSOs)**

  Schedule contractors will have 60 days to accept the mass modification to add FAR 52.204-24 and FAR 52.204-25 to their contracts when it is released this month.

- SOC Reporting for Supply Chain
  Assessing the broader framework of risks to the supply chain may be helpful to organizations as they consider implementing changes to respond to these regulatory updates. The American Institute for Public Accountants (AICPA) is in the process of creating guidance for the creation of System and Organization Controls (SOC) for supply chain. This report would be "an internal control report on an entity's system and controls for producing, manufacturing or distributing goods to better understand the cybersecurity risks in their supply chains."

The AICPA published an exposure draft on the criteria for a description of an entity's production, manufacturing, or distribution system in a SOC for supply chain support. A SOC report for supply chain is designed to provide users with information about the system used to produce, manufacture, or distribute products and the relevant controls within that system (AICPA 2019).

As effective control and oversight of supply chain becomes increasingly difficult for federal contractors, a gap assessment that has been designed appropriately could provide additional assurance and help prevent threats to business continuity. This framework or something similar is something that federal contractors with significant risk in this area may want to consider.

Conclusion

This rule is expected to have a major impact across the Federal supply chain. Failure to properly assess exposure and calibrate systems, polices, and procedures to pivot toward compliance could result in financial and reputational harm, and perhaps even suspension and debarment. The contractor community would be wise to familiarize itself with the rule and understand the implications for ongoing compliance.

For more information on this topic, or to learn how Baker Tilly specialists can help, contact our team.