Professional Perspective

Supply Chain Scrutiny & Government Contracting

Susan Cassidy, Mike Wagner, and Ryan Burnette, Covington & Burling

Bloomberg Law

Supply Chain Scrutiny & Government Contracting

Contributed by Susan Cassidy, Mike Wagner, and Ryan Burnette, Covington & Burling

The federal government—and particularly the Department of Defense (DOD), Department of Homeland Security (DHS), and the intelligence community—are increasingly working to mitigate risks across industrial and innovation supply chains that provide hardware, software, and services to the U.S. government. These steps reflect concerns that a global supply chain has created greater risks of industrial espionage, expropriation of valuable technologies, and exploitation of vulnerabilities in products or services.

In particular, the government is imposing sourcing limitations on contractors—who are expected to provide the first line of defense against supply chain vulnerabilities—and increasingly scrutinizing product development and information security practices of its suppliers.

This article examines domestic preferences in federal government procurement and highlights tools developed by the federal government to eliminate products and sources believed to present a national security risk, including:

- The most significant proposed changes to Buy American Act domestic sourcing requirements in nearly 70 years
- Recent broad restrictions relating to certain covered telecommunications equipment and services under Section 889 of the FY 2019 National Defense Authorization Act (NDAA)
- Forthcoming restrictions on DOD's procurement of printed circuit boards manufactured or assembled in certain covered countries under Section 841 of the FY 2021 NDAA
- The availability of new exclusion tools to the government, including the Federal Acquisition Security Council and Executive Order 13873, the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain."

These requirements, and the severe consequences that for non-compliance that they represent, are discussed here.

Buy American Act Domestic Sourcing Requirements

Current Requirements

Enacted in 1933, the Buy American Act (BAA) requires companies doing business with the U.S. government to formally certify whether end products they deliver under federal contracts are "domestic end products" within the meaning of the BAA and its implementing regulations. In general, a product qualifies as a "domestic end product" if it is manufactured in the U.S. and the cost of its components mined, produced, or manufactured in the U.S. exceeds 55% of the cost of all components.

Although easily stated, the BAA's two-pronged standard frequently is challenging to apply in practice, primarily because the statute neither defines the term "manufacture," nor provides an objective means of distinguishing "components" from "end products."

Moreover, in some circumstances, the standard two-part test will vary, including where the item is being procured by DOD—where components sourced from "qualifying countries" count towards the domestic content threshold—and for commercially available off-the-shelf items, where the only relevant consideration is whether the end items are manufactured in the U.S. Additionally, as of January 2021, there now are also specific limitations with regard to end items composed "predominantly of iron or steel."

Adding to the complexity are a variety of regulatory exceptions and exclusions, in which case the statute may not apply at all. The full set of exclusions is set forth in Federal Acquisition Regulation (FAR) 25.1 and FAR 25.2. The most frequently relied-upon exception applies where the acquisition is subject to the Trade Agreements Act, which waives the requirements of the BAA. This is because the TAA applies to most supply or service contracts whose overall value exceeds a specified statutory threshold, set at $182,000 as of October 2021.

Proposed Regulatory Changes

In July 2021, the government released a proposed rule setting forth the most robust changes to the implementation of the BAA in almost 70 years. This proposed rule is the latest of several actions by the Biden administration aimed at promoting greater economic and national security by supporting domestic manufacturing. Three substantive changes are worthy of particular attention:

Higher Domestic Content Threshold. The proposed rule would initially increase the BAA's domestic content threshold for determining whether an item qualifies as a "domestic end product" from 55% to 60%. It also proposes to increase the threshold to 65% in two years, and to 75% five years after the second increase. There is also a "fallback threshold" exception that would allow end products that meet the current 55% threshold to qualify as "domestic" when other "domestic" products are unavailable or unreasonably expensive.

Enhanced Price Preferences for "Critical" Items & Components. The proposed rule outlines a framework for enhanced price preferences for certain "critical items" and "critical components" manufactured in the U.S. Notably, the proposed rule does not designate any specific articles as "critical," instead, the list of "critical" items and associated preference factors would be set forth in a separate rulemaking.

New Domestic Content Reporting Requirements. The proposed rule also sets forth new domestic content disclosure requirements for "critical items" and end products containing "critical components." Contractors that supply these items would be required to submit a post-award disclosure to the newly established Made in America office identifying the percentage of domestic content in each critical product, and the percentage of domestic content in each domestic end product they supply that includes a critical component.

There is more action to come as the proposed rule moves toward finalization. Public comments were accepted through Oct. 28, 2021, and contractors should continue to closely track developments in this space.

Section 889 of FY 2019 National Defense Authorization Act

Another type of sourcing limitation are product or company bans. For example, in 2018, the DHS issued a directive that banned Kaspersky software and products from government systems. This eventually translated into a ban in the FAR on using Kaspersky products and services on contractor systems and in contractor deliverables.

The Kaspersky ban was a harbinger for Section 889 of the FY 2019 NDAA, which imposes a statutory prohibition on the government from either procuring certain covered telecommunications equipment and services (CTE/S) (Part A), or entering into an agreement with any entity that "uses" CTE/S as a "substantial or essential component of any system, or as critical technology as part of any system" (Part B).

CTE/S is defined under the statute as:

- All telecommunications equipment produced and provided by Huawei Technologies Company or ZTE Corporation and their affiliates or subsidiaries
- Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, and their affiliates or subsidiaries if used for purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes
- Telecommunications or video surveillance services provided by any of the five named companies, their subsidiaries and affiliates, or using equipment from the five companies or their subsidiaries and affiliates

The statute also has provisions for adding new sources, although that has not yet occurred.

The Part B "use" ban has proven especially challenging for contractors. Although the prohibition only applies to companies in direct contractual privity with the U.S. government, "use" extends to commercial and internal uses by those prime contractors. The regulations that implement Part B require a prime contractor to conduct a "reasonable inquiry," as to its use of CTE/S. This is defined to mean "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 that excludes the need to include an internal or third-party audit."

Section 889 had strong support from both sides of Congress. As a result, there are very limited exclusions to the requirements and obtaining waivers has been challenging. Indeed, the waivers that can be issued by the heads of agencies only delay implementation of the requirements and do not permanently exempt contractors of compliance. Agencies are prohibited from issuing Part A waivers that extend past Aug. 13, 2021, and from issuing Part B waivers that extend past August 13, 2022. The Office of the Director of National Intelligence (ODNI) can extend these waivers in limited circumstances. Although a final rule was expected in August 2021, one has not been issued as of the date of this article.

DOD's Printed Circuit Board Prohibitions

Another example of the government's focus on China in the supply chain is Section 841 of the FY 2021 NDAA. Effective Jan. 1, 2023, Section 841 prohibits the DOD from acquiring printed circuit boards (PCBs) from the People's Republic of China, the Democratic People's Republic of North Korea, the Russian Federation, and the Islamic Republic of Iran that perform a mission critical function. The statute defines a PCB as any partially manufactured or completely bare printed circuit board, or fully or partially assembled printed circuit board that performs a mission critical function, but excludes commercial products and services.

The Secretary of Defense may also either designate certain PCBs to be covered by the rule, or waive the prohibition in certain limited circumstances. However, such waivers are expected to be difficult to obtain. Although the provision currently includes the same exclusions as Section 889, including a waiver where the PCB cannot route or redirect user data traffic or permit visibility into any user data or packets, it is not clear how widely such exclusions will apply.

Initial regulations with more implementation details are due by May 1, 2022 unless the current NDAA makes any additional changes. Given the broad range of products that use PCBs, manufacturers with end products that are used by DOD should begin taking steps to comply with these requirements as soon as possible.

New Exclusion Tools

In addition to imposing bans on specified products, the government has developed a number of tools it can use to evaluate national security risks and move to exclude products and services from procurements altogether. Two recent tools implemented by the government are the Federal Acquisition Security Council (FASC) removal and exclusion authorities, as well as the government's authority to impact certain transactions beyond government procurements pursuant to Executive Order 13873 on securing information and communications technology and services supply chain (ICTS EO).

Federal Acquisition Security Council

The FASC has two primary functions. The first is to develop a government-wide strategy for addressing supply chain risks from information and communications technology (ICT) and to facilitate information sharing within the government and outside of the government. The FASC's second function is to establish procedures for the exclusion of ICT products and/or contractors from federal procurements, and the removal of ICT products from federal information systems when it determines that those products present a supply chain risk.

Although the FASC is tasked with recommending exclusion or removal orders, the heads of DHS, DOD, and Office of the Director of National Intelligence (or their delegates) ultimately make the final decision on whether to issue (or rescind) those recommended exclusion or removal orders for the civilian, defense, and intelligence agencies, respectively. If an order is recommended by the FASC, then the FASC or its designee will provide notice of the recommendation to the affected contractor. The contractor then has 30 days to provide a "thorough and complete written response" to the recommendation. After reviewing the information from the FASC and the contractor's response to the FASC allegations, the relevant secretary or director will determine whether to issue an order.

Other than the opportunity to respond to the FASC's recommendation, a contractor's only other opportunity for relief is to bring a lawsuit in the U.S. Court of Appeals for the District of Columbia Circuit. This challenge must be filed within 60 days of being notified of an exclusion or removal order and the government can limit the information that is disclosed in the court action.

Executive Order

The ICTS EO grants the Secretary of Commerce the authority to prohibit certain transactions, including commercial transactions, involving ICTS that have been "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" and that pose an "undue or unacceptable

risk to the national security of the United States." On Jan. 19, 2021, the Department of Commerce (DOC) published an Interim Final Rule to implement provisions of the ICTS EO but there had not been widespread use of the authority yet.

The interim rule identifies a list of governments and a nongovernment person who will be treated as foreign adversaries under the ICTS EO. These are China, Iran, Cuba, North Korea, Russia, and the regime of Venezuelan politician Nicolás Maduro. The interim rule further states that DOC may change this list any time, based on sources including "threat assessments and reports from the U.S. Intelligence Community, the U.S. Departments of Justice, State, and Homeland Security."

Under the rule, DOC may unwind, prohibit, or modify a covered transaction, which generally includes transactions initiated after Jan. 19, 2021 that involve certain enumerated categories of ICTS. For transactions that are identified as falling within the interim rule, the secretary will assess whether to accept, reject or ask more information about the referral.

If the secretary accepts the referral, the secretary will conduct an initial review to assess whether the transaction imposes an "undue or unacceptable risk." If the secretary finds that an ICTS transaction likely meets the criteria of risk, the secretary must notify the appropriate agency heads "and, in consultation with them" determine whether the ICTS transaction is subject to the rule. Finally, the secretary will make an initial written determination explaining why the transaction is subject to the rule, and setting forth whether the transaction should be blocked or other mitigation measures should be taken. DOC will notify the parties to the transaction of the decision by service or through publication in the Federal Register.

Given the significant impact on a variety of transactions, the rule states that DOC will implement a pre-clearance process "to allow a party or parties to a proposed, pending, or ongoing ICTS Transaction to seek a license." The procedures "will establish criteria by which persons may seek a license to enter into a proposed or pending ICTS transaction or engage in an ongoing ICTS Transaction." DOC will review license applications within 120 days of acceptance, and a license will be deemed granted if DOC does not issue a decision within that timeframe. How broadly DOC will rely on this authority remains to be seen.

False Claims Act, Contract Remedies & Suspension and Debarment

When contractors identify a potential noncompliance with the BAA or other sourcing restriction, this can trigger a range of potentially significant consequences ranging from contract breach allegations to violations of the False Claims Act. As to the FCA, the FAR requires federal contractors and subcontractors to make a "timely" written disclosure to the Office of Inspector General for the relevant federal agency whenever they have "credible evidence" of a violation of the civil False Claims Act (FCA) or certain covered criminal statutes in connection with a federal contract.

Regardless of whether a contractor makes a mandatory disclosure, the government can and does actively enforce compliance with sourcing restrictions on its own—especially in the current political environment. Most notably, false representations and certifications about country of origin—whether express or implied—can result in treble damages and cumulative statutory penalties under the FCA. And, in some cases, alleged noncompliance with sourcing requirements can be pursued as a criminal matter under various fraud statutes.

Even aside from traditional enforcement actions, companies can suffer a range of collateral consequences at the contract level, including removal of products from the Federal Supply Schedule, termination of the contract for default, referral to the Office of Inspector General, and negative performance evaluations on government contracts. Finally, companies found to have violated sourcing laws and regulations also may face suspension and debarment from government contracting, which disqualifies companies from bidding on and receiving new federal contracts and subcontracts.

Conclusion

The government has been focused on supply chain integrity and security for more than a decade, but never more so than in the current moment. As the threats have increased, so has the government's scrutiny of its contractors and their suppliers. The government's focus is increasingly aimed at minimizing supply chain security threats from companies that provide it with goods and services dependent on global supply chains.

Increasingly, this scrutiny is focused on particular countries of concern and the government's patience with non-compliance is limited, despite the complexity of these regulations. These actions demonstrate that the government will not hesitate to use all the tools at its disposal if it has a supply chain concern, especially if national security is at risk. Moreover, contractors need to understand these sourcing limitations and implement compliance processes, or they may find themselves at competitive disadvantage or even precluded from competitions.