THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 14 **April 12, 2017**

Focus

¶ 98

FEATURE COMMENT: International Supply Chain Risks And Challenges For U.S. Government Contractors

Supply chain management has become a critical compliance function for Government contractors. With global supply chains, contractors face increased risks and demands. Government contractors must police their supply chains to ensure compliance with U.S. laws, regulations and applicable contract requirements. Moreover, contractors need to identify risks that could affect their reputation or performance capacity.

Legal and contractual issues that arise run the gamut, and include, among others, export controls, U.S. sanctions and embargoes, human trafficking, domestic preference requirements, cybersecurity, counterfeit parts, antiboycott laws, the Foreign Corrupt Practices Act (FCPA), conflict minerals, business ethics and intellectual property. Contractors' supply chain decisions must balance the Government's policy goals against the economic realities that constrain contractors' ability to offer goods and services at a competitive cost or price. While noncompliance can threaten an enterprise's ability to conduct business, so too can cost-prohibitive price hurdles or supply chain scarcity.

As Government contractors expand their supply chains beyond U.S. borders, supply chain risk management is increasingly important and complicated. Contractors working abroad, whether for the U.S. or a foreign government, must be acutely aware of the compliance risks associated with a more diversified and global supply chain, especially as contractors deal with non-U.S. subcontractors and suppliers.

Further, there is a constantly evolving body of laws and regulations that affect how contractors govern their own supply chains, as well as those of their subcontractors. In particular, this body of laws and regulations has seen a proliferation of new developments in recent years. To top it off, contractors' supply chains have been subject to enhanced scrutiny from federal agencies, making supply chain compliance an increasingly critical aspect of contractors' businesses. See Campos, "Government Contracts: Holding Contractors Accountable for the Supply Chain," 29 Westlaw Journal Government Contract 1 (2016).

Additionally, the global nature of supply chains means that contractors doing business around the globe must follow not only U.S. laws, but also foreign laws such as the UK Bribery Act, the UK Modern Slavery Act of 2015 and the European Union's Directive on Transparency. As supply chain enforcement becomes more of a hot topic and supply chains expand beyond U.S. borders, contractors must ensure effective and efficient compliance programs.

This Feature Comment begins by laying out the contractual and regulatory requirements of four critical areas of concern within the supply chain realm: export controls, human trafficking, cybersecurity and domestic preference laws. It then discusses ways in which prime contractors and subcontractors are potentially exposed to risk by their global supply chains. Finally, this Feature Comment concludes by providing guidance to mitigate risks associated with global supply chain management.

Contractual and Regulatory Requirements—Laws, regulations and contractual requirements related to export controls, human trafficking, cybersecurity and domestic preference requirements all have significant implications for supply chain management, particularly as U.S. contractors explore opportunities abroad.

U.S. Export Controls: As U.S. Government contractors contract overseas with greater frequency, they must be aware of compliance risks associated

with U.S. export control laws. The two basic regimes of export control laws are the International Traffic in Arms Regulations (ITAR), administered by the Department of State, and the Export Administration Regulations (EAR), administered by the Department of Commerce. Other international trade embargoes and sanctions pertinent to supply chain management include sanctions administered by the Office of Foreign Assets Control of the Department of the Treasury, and the FCPA, which is administered by the Department of Justice and the Securities and Exchange Commission.

Notably, both the ITAR and the EAR have been interpreted to apply extraterritorially. Extraterritorial jurisdiction is based on the premise that jurisdiction under these regulations "follows the part," and derives from the U.S. nationality of the item or service being exported. See, e.g., Proposed Charging Letter from the Department of State to Intersil Corporation, *www.pmddtc.state.gov/compliance/consent_agreements/pdf/Intersil_%20PCL.pdf*.

Within the supply chain arena, this means that all foreign persons whose activities relate to items or technology under the jurisdiction of the ITAR or EAR, even outside U.S. borders, must be concerned about complying with these regulations. Id. Additionally, and critically important, compliance with the ITAR and the EAR must be flowed down to subcontractors (if applicable), including international subcontractors. 48 CFR § 252.225-7048.

The Department of State's Directorate of Defense Trade Controls, through the ITAR, controls the export of "defense articles," "technical data" and "defense services." The ITAR governs the manufacture, export, temporary import and brokering of defense articles, services and related technical data. 22 CFR pt. 120. Defense articles include hardware and software, as well as related technical data, that are developed, adapted, modified, configured or designed for military application. Id.

The U.S. Munitions List, which is published in the ITAR, contains the 21 categories of ITAR-controlled defense articles and related technical data. Id. All U.S. manufacturers and exporters of ITAR-controlled technology must register with DDTC. Notably, an "export" under the ITAR includes not only the physical movement of a defense article outside the U.S., but also the disclosure (including oral or visual) or transfer of technical data to a foreign person, whether in the U.S. or abroad. 22 CFR § 120.50.

The EAR, on the other hand, is administered by the Department of Commerce's Bureau of Industry and Security. Unlike the ITAR, the EAR regulates the export and import of commercial items, although many of these items are "dual-use" items, which have both commercial and military application. 15 CFR pt. 730. Items controlled by the EAR can be found on the Commerce Control List and are assigned a designated export control classification number based on an item's category. Id. Whereas the ITAR controls an item for all countries, the EAR may control an item for some countries or end users, but not for others. License requirements for items under the EAR depend on the item's characteristics and geographic destination, the end user, and the end use. See 15 CFR § 730.7.

Combating Trafficking Provisions: The rules governing human trafficking are formally known as "combating trafficking in persons" (CTIP) rules, and they are issued under Federal Acquisition Regulation subpt. 22.17 and FAR 52.222-50. 48 CFR subpt. 22.17; 48 CFR § 52.222-50. These rules prohibit a variety of activities related to trafficking persons during recruiting, hiring and employing for both domestic and overseas contract performance, such as using forced labor, using force or the threat of force in hiring, and procuring commercial sex acts. 48 CFR § 52.222-50(b). Notably, FAR 52.222-50 applies to all solicitations and contracts, as designated in FAR 22.1705. 48 CFR § 22.1705(a)(1).

The anti-trafficking regulations were expanded on Jan. 29, 2015, when the FAR Council issued a final rule amending the FAR to implement Executive Order 13627, "Strengthening Protections Against Trafficking in Persons in Federal Contracts," and Title XVII of the National Defense Authorization Act for Fiscal Year 2013. 80 Fed. Reg. 4967 (Jan. 29, 2015). Among other things, by virtue of this final rule, prime contractors and subcontractors, and their employees and agents, must not engage in a range of expanded practices related to human trafficking.

Chiefly, this final rule requires prime contractors to certify implementation of compliance plans to combat human trafficking, and to flow down these certification requirements to subcontractors if a subcontract exceeds certain threshold requirements. In particular, if a non-commercially available off-the-shelf (non-COTS) contract or subcontract outside the U.S. exceeds $500,000, a prime contractor must certify that

> [i]t has implemented a compliance plan to prevent any prohibited activities identified in

> paragraph (b) of the clause at 52.222-50, Combating Trafficking in Persons, and to monitor, detect, and terminate [any agent, subcontract or subcontractor employee] engaging in prohibited activities identified at paragraph (b) of the clause at 52.222-50, Combating Trafficking in Persons.

48 CFR § 52.222-50(h).

In essence, therefore, contractors and subcontractors that provide supplies acquired abroad, or perform services outside the U.S., on contracts or subcontracts worth over $500,000 must implement a compliance plan and complete compliance certification before they may receive a contract award. Further, contractors must complete such certification annually during contract performance. 48 CFR § 52.222-50(h)(5).

As is the case with export control laws, compliance with CTIP rules is flowed down to subcontractors. 48 CFR § 52.222-50(i). This fact is critically important for U.S. prime contractors and both domestic and foreign subcontractors as they prepare supply chain compliance programs.

Domestic Preference Laws: Similar compliance issues abound with respect to domestic preference laws such as the Buy American Act (BAA), 41 USCA §§ 8301–8305, and the Trade Agreements Act (TAA), 19 USCA §§ 2501–2581. The BAA requires the U.S. to offer preferential treatment to "domestic end products" in certain federal procurements and contract awards. This preferential treatment is implemented through price preferences for domestic offers (i.e., offers consisting of domestic end products or domestic construction materials).

The TAA, on the other hand, is basically an exception to the BAA, and permits the Government to purchase products and services on a nondiscriminatory basis from designated countries that have signed trade agreements with the U.S. The TAA, therefore, permits the Government to acquire U.S.-made *or* designated country end products for use on Government contracts in certain circumstances.

Both the BAA and the TAA have certification requirements. To illustrate, as prescribed in FAR 25.1101(a)(2), the following provision must be inserted into contracts covered by the BAA: "The offeror certifies that each end product, except those listed in paragraph (b) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States." 48 CFR § 52.225-2. Similarly, as prescribed in FAR 25.1101(c)(1), the following provision must be inserted into contracts covered by the TAA: "The offeror certifies that each end product, except those listed in paragraph (b) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled 'Trade Agreements.' " 48 CFR § 52.225-6. These certification requirements impose the potential to incur False Claims Act liability (discussed infra).

Language in the FAR does not expressly dictate that compliance with the BAA or the TAA is flowed down to subcontractors; however, prime contractors seeking to obtain supplies from subcontractors under BAA- or TAA-subject contracts will naturally seek to flow these compliance requirements down, and they often require certifications from their subcontractors.

Cybersecurity: Government contractors are subject to a rapidly developing array of cybersecurity regulations, predominately implemented by the Department of Defense. These regulations have significant implications for supply chain risk management because contractors and subcontractors must safeguard covered information throughout the supply chain.

DOD issues rules regarding the safeguarding of covered defense information, which encompasses, among other categories, unclassified controlled technical information and controlled unclassified information. The complicated web of rules in this area essentially requires contractors to safeguard certain protected information and report cyber incidents, which are attacks on or potential compromises to covered information.

Of particular relevance to supply chain management is DOD's final rule, published Oct. 30, 2015, that, among other things, amended the Defense Federal Acquisition Regulation Supplement to include subpt. 239.73, Requirements Relating to Supply Chain Risk. 80 Fed. Reg. 67243 (Oct. 30, 2015). First, this final rule requires DOD to use supply chain risk as an evaluation factor for covered contracts in determining contract award. Second, it enables DOD to exclude a contractor from procurements related to national security systems if it finds risks in the contractor's supply chain. Id. Ultimately, the final rule relates to cybersecurity because contractors that provide DOD with "information technology, whether as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system,"

must mitigate supply chain risk to the supplies and services being provided to the Government. Id.

Risk Exposure via Global Supply Chains—The array of laws, regulations and emerging contractual requirements in supply chain management can prove to be a minefield for contractors and subcontractors as they attempt to formulate supply chain compliance programs. The problem is exacerbated when contractors explore opportunities abroad. Two areas of particular risk for global supply chains are the extraterritorial application of U.S. laws and contractual issues applicable to the four areas discussed above (including FCA liability).

Extraterritorial Application of U.S. Laws: With use of global supply chains on the rise due to economic globalization, integration and convergence, contractors exploring overseas work must appreciate the significant risks posed by the extraterritorial application of U.S. laws. For example, the regulatory requirements of both the ITAR and the EAR apply overseas because—as explained above—U.S. jurisdiction follows an article or technology, wherever it is located in the world. Thus, subsequent transfers of an ITAR- or EAR-controlled article or technology, even after its initial export from the U.S., can lead to a violation of the applicable regulation.

As a consequence, contractors must secure relevant authorizations before such items are exported (or reexported or retransferred by a subcontractor outside the U.S.), and monitor subcontractor handling of such items. To illustrate, in June 2014, Intersil Corporation entered into a settlement (consent agreement) with the State Department after it was charged with 339 violations of the Arms Export Control Act and the ITAR. Proposed Charging Letter from the Department of State to Intersil Corporation, *www.pmddtc.state.gov/compliance/consent_agreements/pdf/Intersil_%20PCL.pdf*. A major issue highlighted in the State Department's proposed charging letter was the fact that unauthorized exports were subsequently reexported or retransferred by a foreign company overseas without U.S. authorization. In other words, ITAR-controlled items were retransferred by Intersil customers *within* certain foreign countries, and, on at least 91 occasions, reexported from those foreign countries to China, without proper authorization from the U.S. Government. Id.

Similarly, U.S. anti-trafficking provisions apply extraterritorially. See generally 48 CFR § 52.222-50. Particularly, as required by 48 CFR § 52.222-50(h), contractors must maintain compliance plans regarding U.S. anti-trafficking laws if any portion of a contract is to be performed outside the U.S., and the estimated value of that portion exceeds $500,000. 48 CFR § 52.222-50(h). Given that the CTIP provisions of the FAR must be inserted in all solicitations and contracts, and given that compliance with the provisions must be flowed down to subcontractors, paragraph (h) has far-reaching ramifications for contractors' global supply chains. For example, any time a contractor works abroad on a contract worth over $500,000, it must have a compliance plan to satisfy the U.S. CTIP provisions.

The CTIP provisions are designed to implement the Trafficking Victims Protection Act (TVPA) of 2000 and subsequent reauthorizations. 48 CFR subpt. 22.17; 22 USCA chap. 78. Notably, although the original TVPA did not apply extraterritorially because jurisdiction was limited to trafficking activity "in or affecting interstate or foreign commerce," Congress subsequently amended the TVPA to authorize extraterritorial jurisdiction. See 18 USCA § 1596(a) (2008); *Aguilera v. Aegis Commc'ns Grp.*, LLC, 72 F. Supp. 3d 975, 979 (W.D. Mo. 2014); *Plaintiff A v. Schair*, No. 2:11-CV-00145-WCO, 2014 WL 12495639, at *1 (N.D. Ga. Sept. 9, 2014).

Importantly, however, the TVPA's extraterritorial application does not apply retroactively to pre-2008 conduct. *Plaintiff A v. Schair*, 2014 WL 12495639, at *3. Nevertheless, the TVPA provides innovative solutions for eradicating human trafficking, even abroad, because it sets "minimum standards for the elimination of trafficking" applicable to governments of countries that are places of "origin, transit, or destination for ... victims of ... trafficking." 22 USCA § 7106.

For example, in *Plaintiff A v. Schair*, although extraterritorial jurisdiction was not applied retroactively to alleged instances of trafficking acts that occurred outside the U.S. and entirely within Brazil, the court noted that Congress's passage of 18 USCA § 1596 made the TVPA expressly extraterritorial in 2008. *Plaintiff A v. Schair*, 2014 WL 12495639, at *3; see also *Adhikari v. Daoud & Partners*, 994 F. Supp. 2d 831, 835 (S.D. Tex. 2014).

Contractual Issues: In addition to the extraterritorial application of U.S. laws, which can have significant ramifications for U.S. prime contractors and subcontractors, there are a host of contractual issues that plague a global supply chain. One area of concern for prime contractors and subcontractors alike

is flowdown requirements. Contractual requirements flow down, in many cases, to subcontractors, even ones based overseas. For example, in addition to the extraterritorial application of U.S. laws, compliance with U.S. export control laws and U.S. anti-trafficking laws is mandatorily flowed down as a contract requirement to subcontractors, including international subcontractors. See 48 CFR § 252.225-7048; 48 CFR § 52.222-50(i).

Additionally, prime contractors under BAA- or TAA-subject contracts will naturally seek to flow down country-of-origin requirements, and they often seek certifications from their subcontractors. Safeguards for covered defense information must be flowed down to subcontractors as well. 48 CFR § 252.204-7012(m). As a consequence, subcontractors must be judicious in setting up supply chain compliance programs to protect themselves from U.S. Government enforcement and prime contractor-subcontractor disputes.

The negative ramifications of noncompliance are far-reaching and can be crippling to an organization. Consequences of noncompliance with contractual provisions can include breach of contract and corresponding damages, termination for default or convenience, or suspension or debarment—all of which could limit the ability of a contractor (or subcontractor) to get contracts in the future. Further, contractual certifications raise problems regarding the FCA. In fact, supply chain management issues have become an increasing hotbed of FCA enforcement activity over the last several years.

In particular, the FCA has been used to combat false certifications related to U.S. export control laws, human trafficking, country-of-origin requirements of the BAA and TAA, and cybersecurity. As the primary tool to rectify false claims for Government property and funds under Government contracts, the U.S. has relied heavily on the FCA to ensure Government contractors' compliance. In fact, DOJ recovered more than $4.7 billion in FCA settlements and judgments in FY 2016, which is the third-highest annual recovery in FCA history. DOJ, Office of Public Affairs, "Justice Department Recovers Over $4.7 Billion From False Claims Act Cases in Fiscal Year 2016," Dec. 14, 2016. Of that $4.7 billion recovered by the Government, $2.9 billion arose from the 702 lawsuits filed under the qui tam provisions of the FCA. Id.

Importantly for Government contractors, exposure to FCA liability is not confined to a prime contractor's own business organization. Rather, the Government can hold a prime contractor liable under the FCA as a result of false claims initially submitted by, or false certifications or statements initially made by, a subcontractor. This stems predominately from two facts: (1) "Knowingly" under the FCA is defined as including acting with deliberate ignorance as well as acting with reckless disregard; and (2) some courts have interpreted the FCA broadly such that it imposes liability under a theory of implied certification, whereby a claim for payment to the Government contains an unexpressed certification of compliance with material contract terms or regulations. 31 USCA § 3729(b)(1)(A); *U.S. ex rel. Augustine v. Century Health Servs., Inc.*, 289 F.3d 409, 415 (6th Cir. 2002); *Ebeid ex rel. U.S. v. Lungwitz*, 616 F.3d 993, 996–98 (9th Cir. 2010); *U.S. ex rel. Wilkins v. United Health Grp., Inc.*, 659 F.3d 295, 306 (3d Cir. 2011).

Given that FCA liability arises as a result of knowingly making a false certification to the Government, regulations that require certification heighten the threat of FCA liability. This is the case for U.S. export controls, human trafficking regulations, the BAA and TAA country-of-origin requirements, and cybersecurity regulations. See, e.g.:

- Department of Justice, Office of Public Affairs, "Wisconsin Architectural Firm to Plead Guilty and Pay $3 Million to Resolve Criminal and Civil Claims," Jan. 5, 2016 (Wisconsin-based architectural firm Novum Structures LLC pled guilty to resolve civil allegations under the FCA that it caused false claims to be submitted to the Government for payment by knowingly using noncompliant foreign materials on several federally funded construction projects in violation of the BAA);
- *U.S. ex rel. Sheldon v. Kettering Health Network*, 816 F.3d 399 (6th Cir. 2016) (court rejected relator's FCA claim, but it did not question that a failure to comply with cybersecurity requirements could give rise to FCA liability); 58 GC ¶ 91;
- Department of Justice, Office of Public Affairs, "Rocky Mountain Instrument to Pay U.S. $1 Million to Resolve False Claims Act Allegations," Oct. 29, 2010 (Rocky Mountain Instrument Company (RMI) settled for $1 million regarding allegations that RMI violated the FCA by submitting claims for payments to various defense prime contractors, who had, in turn, claimed reimbursement for optical and

laser products manufactured overseas using sensitive technical data exported by RMI in violation of the ITAR).

As a consequence, Government contractors should build strong compliance programs in these areas to prevent a violation of the FCA.

Conclusion—Given recent enforcement trends, federal contractors must be on guard. The risks associated with managing a supply chain create incentives to patrol, investigate and prevent noncompliance. Both prime and subcontractors should become familiar with U.S. export control laws, anti-trafficking provisions, domestic preference requirements, cybersecurity rules, and other laws and regulations applicable to the supply chain. Prime contractors must exercise due diligence in the supplier selection process to ensure that suppliers comply with contractual agreements as well as applicable laws and regulations.

Further, prime contractors must make sure that subcontractors can perform their assigned tasks. In establishing a supply chain risk management program, contractors also should confirm potential subcontractors' qualifications, and put in place mechanisms to monitor subcontractors. Before selecting a subcontractor, prime contractors should determine a subcontractor's willingness and ability to fulfill reporting obligations. Most importantly, to monitor subcontractors effectively, prime contractors must have a well-trained workforce that actively engages with subcontractor personnel so that red flags will be detected as soon as they arise.

Additionally, diversification of subcontractors in a prime contractor's supply chain helps to solve the systemic risk of supply chain overlap. Diversification also creates enhanced opportunities for beneficial economic growth in the form of greater small business participation and streamlined acquisitions through nontraditional Government contract procurement vehicles. Moreover, nontraditional Government contractors can break into the supply chain with progressive procurement strategies, vehicles and techniques (e.g., other transaction agreements) that simultaneously reduce the risks created by supply chain overlap.

The risks and demands associated with global supply chains are high. Ensuring compliance with all applicable laws, regulations and contractual terms in an ever-changing environment can seem daunting. To avoid pitfalls, contractors should establish a formal written compliance program, constantly engage in due diligence and risk assessment, employ careful recordkeeping and training processes, and create templates for contracts and agreements so that appropriate terms and provisions are flowed down.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Kevin Lombardo *and* Norman Aspis*, members of Dentons US Government Contracts and Global Public Procurement Practice. Kevin Lombardo is a Partner in Los Angeles, where he focuses his practice on international trade regulations and Government contract law, counseling US and non-US parties regarding matters involving the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), sanctions imposed by the Office of Foreign Assets Control (OFAC), the US anti-boycott regulations, the regulations imposed by the Committee on Foreign Investment in the US (CFIUS), and the Foreign Corrupt Practices Act (FCPA). Norman Aspis is an Associate in the Los Angeles office, where his practice covers a wide range of Government contracts matters, with an emphasis on export controls.