Steptoe

STEPTOE & JOHNSON LLP

The Government Contractor Supply Chain Toolkit

Version 2.0

December 22, 2016

TABLE OF CONTENTS

The Government Contractor Supply Chain Toolkit

I. Introduction

A. Why a Supply Chain Toolkit?

Supply chains are receiving a great deal of attention. What once was known simply as a company's "purchasing function" has evolved into an important compliance function for all companies and particularly for government contractors. Supply chain management is now a key element to ensuring a company's compliance with laws, regulations, and its internal policies, and to identifying risks that could impact a company's ability to perform, as well as its reputation.

The fact that supply chains are global increases the risks and demands on companies. Government contractors are now being asked to effectively police their supply chains to address, among other risks, counterfeit parts, human trafficking, business ethics, and cyber threats. They also may be required to make supply chain decisions to support certain socio-economic and domestic preference goals identified by the Government. Meanwhile, those same contractors must make supply chain decisions that enable them to offer their goods and services at a competitive cost or price in order to receive award.

For example, concern over counterfeit parts in the defense supply chain resulted in a rule that mandates the creation of procedures to monitor, detect, and eliminate counterfeit parts. Noncompliance threatens the enterprise's ability to conduct business. Also, the rule that seeks to eliminate trafficking in persons mandates the creation of procedures to effectively address the trafficking risk through monitoring the supply chain. We are also seeing a convergence of cybersecurity risk mitigation and supply chain processes due to the increased risk to companies from "back door" cyberattacks that could come through a company's supply chain.

Contractors can be excluded from government contracting due to supply chain risks. For example, the Department of Defense (DoD) has amended the Defense Federal Acquisition Regulation Supplement (DFARS) to introduce a new DFARS Subpart 239.73 addressing "Requirements for Information Relating to Supply Chain Risk." This Subpart is an attempt to address cybersecurity concerns related to defense contractors and is part of a growing number of national and agency-level supply chain initiatives. Among other things, it authorizes officials in DoD to exclude certain sources from providing information technology, either as a service or a supply, or to direct DoD contractors to exclude certain sources as subcontractors. Therefore, contractors that directly or indirectly provide IT products or services to DoD must examine the security of their supply chains to maintain their continued eligibility to be awarded contracts.

The Intelligence Community has, in fact, implemented a comprehensive supply chain management program through a Directive called "Supply Chain Risk Management," which "establishes Intelligence Community (IC) policy to protect the supply chain" and defines "supply chain risk management" as "the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain." Although limited to the Intelligence Community, this Directive reflects the Government's growing concern about supply chains in general.

At the same time, there is at least some Congressional awareness of the potential adverse impacts of increasing supply chain requirements on federal contractors and subcontractors. In passing the National Defense Authorization Act ("NDAA") for Fiscal Year 2017, Congress included a provision (Section 887) calling for the review of contractual flow-down provisions in the federal supply chain. Section 887 requires the Secretary of Defense, through an independent entity, to review the necessity and effects of contractual flow-down provisions related to major defense acquisition programs on contractors and suppliers. The Section specifically requires DoD to, *inter alia*, (i) identify FAR and DFARS clauses that flow-down into the supply chain; (ii) indicate which of them are critical for national security; (iii) examine the extent to which flow-down clauses in DoD contracts are applied inappropriately in the subcontracts; (iv) assess unnecessary costs and burdens of those provisions on the supply chain; and (v) determine the effect, if any, of such flow-down provisions on the participation rate of small businesses, contractors for commercial items, nontraditional defense contractors, universities, and not-for-profit research organizations in defense acquisition efforts. The NDAA requests a report addressing the findings of this review and proposed actions to take in response.

B. Scope of the Toolkit

This Toolkit discusses many of the key current and emerging requirements in supply chain management and seeks to aid companies in understanding the importance of supply chain management. It should be noted, however, that this Toolkit does not attempt to be all encompassing. There are many other important issues that can affect the supply chain, especially in traditional areas, such as flow down requirements, The Truth in Negotiations Act (TINA), and other cost accounting areas, that are addressed only peripherally in this Toolkit. Some of these topics may be added in the future, along with new "policing" requirements that the Government may impose from time to time for contractors to monitor or manage their supply chain.

The Toolkit also includes a summary of some critical risk management issues observed by attorneys at Steptoe & Johnson LLP. It does not and cannot, however, address every risk issue, although it does seek to identify the basic standards for compliance. Likewise, it does not contain a comprehensive description of the "best practices" followed by experienced, highly responsible contractors, as those often exceed the minimum standards by a wide margin and will depend on various factors such as the nature of the contracts involved and the particular contractors' (and subcontractors') risk tolerance profiles.

C. 2016 Update

In this 2016 update (Version 2.0), the Toolkit provides an update on various federal rules and developments imposing supply chain requirements on federal contractors and subcontractors. The updated Toolkit includes:

- Updates on newly-issued employment requirements, such as rules addressing the "Fair Pay and Safe Workplaces" and "Paid Sick Leave for Federal Contractors;"
- A snapshot of the major – and fast evolving – cybersecurity requirements;
- Other regulatory updates on human trafficking, counterfeit parts, the expanded scope of the SBA's Mentor-Protégé program for all "small" businesses, and new methods

for calculating limitations on subcontracting for contracts set aside for "small" businesses; and

- Recent civil and criminal enforcement activities by the federal government arising from supply chain risks, including in the areas of illegal kickbacks, counterfeit parts, and the Trade Agreements Act.

Although the conventional wisdom seems to suggest that the new Administration will roll back some of the Obama administration's initiatives in the government's supply chain, such as certain Executive Orders imposing employment-based requirements, there is no question that supply chain risk management will continue to be a key element of compliance programs for government contractors. Despite differences in political views, for example, the federal government will continue its emphasis on increasingly stricter requirements for cybersecurity in the supply chain, particularly in light of recent reports of Russian and Chinese hacking.

For more information, Steptoe's supply chain points of contact for government contractors are Paul Hurst, Tom Barletta, Kendall Enyard, Andy Irwin, Sharon Larkin, Mike Mutek, Mike Navarre, and Fred Geldon or please visit Steptoe's Government Contracts Group website. The contributors to Steptoe's Government Contractor Supply Chain Toolkit also include Jack Hayes, Anthony Rapa, Raquel Parker, and Peter Wellington, as well as editor, Justin Witt.

II. General Considerations: Supply Chain Risk Management

In general, supply chain risk management is an increasingly critical area for government contractors. This is reflected in regulations providing for government reviews of contractor purchasing systems and other regulations imposing affirmative obligations that increase the need for due diligence in supplier selection and effective supply chain management.

A. Contractor Purchasing System Review

Under certain contracts, the US Government evaluates supply chain risks based on its Contractor Purchasing System Review (CPSR). The CPSR is defined in FAR 44.101 as the complete evaluation of a contractor's system for the purchasing of material and services, subcontracting, and subcontract management from development of the requirement through completion of subcontract performance. The purpose of such a review is to evaluate the efficiency and effectiveness with which a contractor spends government funds, and complies with government policy when subcontracting. It also provides the Administrative Contracting Officer (ACO) with the basis for granting, withholding, or withdrawing approval of contractor's procurement system.

In addition, a government contractor's supply chain system, often referred to by the Government as a "purchasing system," constitutes an important business system. Since issuance of the "business systems rule" by the Defense Department in 2011, certain contractors are facing the risk that a contracting officer may find one or more of their business systems noncompliant due to a "significant deficiency." In addition to mandatory penalties, a "significant deficiency" could increase the time and cost of contracting with the Government because additional approvals and oversight may be required.

Under FAR 44.302, a determination to conduct a CPSR is triggered when a contractor's sales to the government are expected to exceed $25 million during the next 12 months. Because a contractor's purchasing system is a business system, the DFARS Business Systems Rule, 252.244-7001(a), contains the 24 criteria required to exist in all contractor purchasing systems in order to be deemed an acceptable system. Importantly, if the ACO deems that a purchasing system is significantly deficient in any one of the 24 criteria, the system will be deemed "unacceptable" according to DFARS 252.244-7001(a).

Generally, a CPSR will evaluate the contractor's purchasing policies and procedures to make sure they cover all the needed requirements, and then audit a sample of purchasing files to determine whether those procedures have been followed. During the CPSR, special attention is given to certain areas identified in FAR 44.202-2 and FAR 44.303, including:

- Market research;
- Degree of price competition;
- Pricing policies and techniques;
- Planning, award, and management of major subcontracts;

- Inclusion of appropriate flow down clauses;
- Appropriateness of types of subcontracts used;
- Methods of evaluating subcontractor responsibility, including use of the System for Award Management (SAM) Exclusions and, if the contractor has subcontracts with parties on the Exclusions list, the documentation, systems, and procedures the contractor has established to protect the Government's interests;
- Policies and procedures pertaining to small business subcontracting program;
- Treatment accorded affiliates and other concerns having close working arrangements with the contractor;
- Compliance with Cost Accounting Standards (if applicable) in awarding subcontracts;
- Management control systems to administer progress payments; and
- Implementation of higher-level quality standards.

A successful CPSR will result in the contractor's purchasing system being "approved". This can be very important to the contractor's ability to conduct its business, because without an approved purchasing system, Contracting Officer consent to the subcontract will be required for cost-reimbursement, time-and-materials, labor hours, or letter contracts, and also for unpriced actions under fixed-price contracts that exceed the simplified acquisition threshold.

The areas evaluated during the CPSR provide a useful checklist for all contractors. The creation of policies and procedures to address these areas is a prudent step in the creation of a strong supply chain management system and the mitigation of risk through evaluation of potential suppliers.

B. Other Risk Management Concerns

A company's supply chain must accomplish a number of important business objectives, but it also, in many ways, serves a compliance function. As a result, contractors should develop processes to ensure compliance and to identify risks in their supply chain. Risk management should serve as an early warning radar to the company and identify potential issues that could impact the company's ability to meet its contractual obligations.

The fact that, on average, the supply chain accounts for over half of most companies' total expenditures attests to the importance of supply chain risk management. This Toolkit highlights other important risk management considerations and makes it clear that a company must first conduct due diligence in the selection of its suppliers and then actively police its supply chain to successfully address these considerations. These risks include the potential for counterfeit parts entering the supply chain, the risk of human trafficking, and the presence of cyber threats, and the failure to meet socio-economic and domestic preference goals.

Other risks that accompany supply chains include disputes, claims, litigation, imputation of wrong-doing to the prime, potential review for suspension or debarment of companies in the supply chain, and reputational damage from having a bad actor in the supply chain. Companies benefit from the creation of clear, understandable policies and procedures that address how to conduct an adequate review of suppliers, particularly new suppliers, and how to ensure that adequate oversight of the supplier continues throughout performance.

C. A Few Words on Risk Implications for the Prime Contractor

A prime contractor's risk exposure often extends beyond the confines of its business organization. An important example of this risk is the civil False Claims Act (FCA). *See* 31 U.S.C. § 3729. The FCA is the primary remedy available to the United States to redress false claims for government funds and property under government contracts. Not only does it impose liability on contractors for knowingly presenting to the Government a false claim for payment but it also could impose liability on contractors for knowingly causing the submission of a false claim for payment or making or using false records or statements material to a false claim. Although the FCA applies to acts committed "knowingly," this term is defined to impose liability on acts taken with actual knowledge of falsity as well as those taken with "reckless disregard" or "deliberate ignorance" of the truth or falsity of the information. Some courts also have interpreted the FCA broadly (perhaps overly so) to impose liability under a theory of "implied certification," the theory that, under certain circumstances, a claim for payment carries with it an unexpressed certification of compliance with material contract terms or regulations.

As a result, under the FCA, there are a number of potential scenarios where the Government could argue that it paid a claim or reimbursed the prime contractor based on false claims initially submitted by, or false statements or certifications initially made by, a subcontractor. For example, there are certain contracts where a prime contractor's proposal or invoices rely or repeat a subcontractor's statements, representations, or certifications. The prime contractor must therefore be alert for red flags or potential issues and consider taking other steps to ensure that any such reliance is reasonable under the circumstances and the broad definition of "knowingly." Some prime contractors also seek to require suppliers to indemnify them for liability arising under the FCA due to false claims or statements made by the supplier. Although a supplier submitting false information to the prime contractor or higher tier subcontractor may be liable for doing so under the FCA, the prime contractor may also find itself exposed under the FCA for the subcontractor's conduct.

D. Vetting Suppliers

It is not surprising that a globally dispersed supply chain includes risks. A company should manage its suppliers wherever they may be located and mitigate these risks by ensuring that suppliers are complying with the terms of their agreements as well as applicable laws and regulations. Contractors should spend time and money in monitoring and enforcing compliance with these agreements, laws and regulations.

Prime contractor obligations have increased in the area of ensuring that its suppliers are properly trained and can perform. Due diligence in the selection of potential suppliers is critical; it is a component of the CPSR and a prudent practice in all situations. There are resources that

can help vet supply chains, including information available in this Toolkit. There is also value in "kicking the tires" and visiting potential suppliers to ensure that they possess the ability to perform. A basic supply chain risk management program should address three key points, which are (1) identify and confirm the qualifications of a potential supplier, including its business reputation and responsibility, (2) confirm the business need and justification for working with the potential supplier, and (3) determine how to conduct ongoing monitoring of the supplier. Contractors should evaluate suppliers' willingness to accept the necessary flow down clauses required by the FAR, the supplier's ability and willingness to fulfill its reporting obligations and otherwise cooperate with the prime contractor, and the supplier's willingness to allow access to its own supply chain.

III. Competitive Considerations: Subcontractor Responsibility and Past Performance in Sourcing

A. Subcontractor Responsibility

Supplier selection is important for all companies, but it is particularly important for government contractors. The Government has extensive source selection processes that are used to select prime contractors. But the Government also wants to be sure that its prime contractors use only qualified and "responsible" suppliers on government contracts. Although the Government has privity of contract, which is a direct legal relationship, with its prime contractors, it does not have privity – or the associated contractual rights – with a prime contractor's subcontractors and suppliers. Accordingly, the Government's consideration of a prospective prime contractor's technical and management abilities may include an assessment of the prime contractor's ability to select and manage the suppliers it proposes to use in the performance of the contract.

Prime contractors are primarily responsible for conducting adequate due diligence on potential suppliers and for the award and administration of subcontracts in support of the prime contract. However, the Government, through its Contracting Officers (COs) and oversight agencies, can play an important role in supplier selection and in supplier oversight. For example, FAR Part 44 (Subcontracting Policies and Procedures) includes provisions requiring, under certain contracts, the prime contractor to obtain CO consent to select a subcontractor, unless the contractor has an Approved Purchasing System. Where CO consent is required, FAR 44.202-2 lists several factors the CO must review and evaluate before granting consent. These include technical need for the services or supplies, compliance with the prime contract's goals for subcontracting with small disadvantaged business and women-owned business concerns, adequacy of competition, responsibility of the proposed subcontractor, proposed type and terms of the subcontract, and adequacy and reasonableness of cost or price analysis performed.

Suppliers may play an important role in the competition for the award of prime contractors. They often provide key technical capabilities and assist in the development of a competitive cost volume or even the preparation of the technical proposal. As noted in the section on teaming arrangements, competition today is often between teams of companies. In such cases, source selection officials are likely to consider the management abilities of the prime contractor and the combined technical capabilities of the entire team – the prime contractor and its suppliers.

That said, prime contractors must avoid the potential for anticompetitive behavior in the selection of suppliers. The selection of a supplier must be for a legitimate purpose and not for the purpose of eliminating competition. COs are wary of joint bids by contractors that could each perform the contract separately, and are alert for unusual or restrictive bidding patterns that may indicate the possibility that contractors may have agreements with other contractors not to compete or bid against each other for a prime contract.

B. Responsibility Considerations

When selecting subcontractors, prime contractors should identify any issues with the subcontractor's "responsibility," such as repeated performance problems or ethical lapses, that could hinder the prime contractor's ability to win award of the contract or successfully perform the contract.

FAR 9.103(a) states that "Purchases shall be made from, and contracts shall be awarded to, responsible prospective contractors only." The term "responsible prospective contractor" is defined as a contractor that meets the standards in FAR 9.104, and the FAR makes clear that prime contractors should consider these same standards in evaluating and selecting subcontractors.

FAR 9.104-4(a) notes that:

> Generally, prospective prime contractors are responsible for determining the responsibility of their prospective subcontractors. . . . Determinations of prospective subcontractor responsibility may affect the Government's determination of the prospective prime contractor's responsibility. A prospective contractor may be required to provide written evidence of a proposed subcontractor's responsibility.

Although FAR 9.104-4(a) makes prime contractors responsible for determining the responsibility of proposed subcontractors, FAR 9.104-4(b) also permits the CO to directly determine the present responsibility of a potential subcontractor where it is in the Government's interest to do so.

The FAR standards for determining responsibility are important to government contractors for two reasons. First, prime contractors should consider the standards as a starting point for their own due diligence review of a potential supplier. Second, a prime contractor is well advised to include language in any supplier agreement that allows termination if a later determination is made that the potential supplier lacks present responsibility. Where a teaming agreement is used, this contingency should be addressed in the agreement. Of course, such a determination could negatively impact the prime contractor's ability to be selected for award, which reinforces the need for due diligence in supplier selection

So what are these FAR responsibility standards? The contractor (and therefore any subcontractor) must:

- Have adequate financial resources to perform the contract, or the ability to obtain them;
- Be able to comply with the required or proposed delivery or performance schedule, taking into consideration all existing commercial and governmental business commitments;
- Have a satisfactory performance record;

- Have a satisfactory record of integrity and business ethics;

- Have the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them (including, as appropriate, such elements as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by the prospective contractor and subcontractors);

- Have the necessary production, construction, and technical equipment and facilities, or the ability to obtain them; and

- Be otherwise qualified and eligible to receive an award under applicable laws and regulations.

Finally, in procurements where the contract value exceeds $30,000, contractors must comply with FAR 52.209-6 ("Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment"). This clause provides that, other than a subcontract for a Commercial Off-the-Shelf (COTS) item, a prime contractor may not enter "into any subcontract, in excess of $30,000" with an entity "that is debarred, suspended, or proposed for debarment by any executive agency unless there is a compelling reason to do so." It also commits prime contractors to require certain prospective subcontractors to disclose "whether as of the time of award of the subcontract, the subcontractor, or its principals, is or is not debarred, suspended, or proposed for debarment by the Federal Government." To the extent that the prime contractor still intends to enter into a subcontract with a debarred or suspended party (other than one providing a COTS item), then the prime contractor must provide advance written notice to the CO, in accordance with this clause. As a result, in practice, prime contractors and subcontractors should implement internal controls for confirming and documenting the status of prospective subcontractors as to suspension and debarment and, if necessary, providing the written notice to the CO.

C. Past Performance Considerations

FAR 15.304(c) makes past performance a factor in almost all source selections, and FAR 42.15 includes detailed provisions for collecting and maintaining contractor performance information. Past performance information of proposed subcontractors, particularly key subcontractors, can be an important part of an offeror's overall past performance rating.

Since 2010, the FAR has required the use of the Federal Awardee Performance and Integrity Information System (FAPIIS). FAPIIS consolidates information from the Excluded Parties List System (EPLS), the Past Performance Information Retrieval System (PPIRS), and the Contractor Performance Assessment Reporting System (CPARS). It also collects information from government contractors, including CO non-responsibility determinations, contract terminations for default or cause, agency defective pricing determinations, administrative agreements entered into following a resolution of a suspension or debarment, and contractor self-reporting of criminal convictions, civil liability and adverse administrative proceedings. Since then, the Government has also implemented the System for Award

Management (SAM) at www.sam.gov, for the purpose of consolidating the government-wide acquisition and award support systems, including FAPIIS and EPLS, into one new system.

The purpose of a single database is to enable COs throughout the Government to monitor the integrity and past performance of companies performing Federal contracts, grants, and cooperative agreements. FAR 9.104-6(a) also provides that, "[b]efore awarding a contract in excess of the simplified acquisition threshold," the CO "shall review" FAPIIS as part of its responsibility determination as well as source selection evaluation of past performance. The publicly-available portions of SAM and FAPIIS include the Excluded Parties List System but do not include past performance information compiled (in PPIRS and CPARS) about other companies. Therefore, prime contractors can obtain this information only from proposed subcontractors themselves. Prior to relying on a subcontractor's past performance, a prime contractor would benefit from a review of a potential supplier's past performance history and the Excluded Parties List, particularly when contracting with a new supplier with which the prime contractor has not previously conducted business.

D. Other Supplier Source Selection Considerations

Prime contractors must comply with FAR 52.244-5, "Competition in Subcontracting," if the clause is included in the contract, and select suppliers on a competitive basis, to the maximum practical extent, consistent with the objectives and requirements of the contract. COs may accept justifications for sole source awards if the prime contractor provides substantive evidence that no other responsible party exists, or there are circumstances of unusual and compelling urgency. Statements by a Prime Contractor to justify a non-competitive subcontract award based on the unique position or characteristics of the subcontractor, such as the geographical location, site specific experience, or that the supplier is the only available source, are unlikely to be an acceptable justification for sole source subcontracting unless adequate documentation is submitted by the prime contractor.

IV. Business Ethics in the Supply Chain

Most contractors and their business partners have long-standing inherent commitments to high standards of business ethics and conduct independent of, and generally stronger than, the standards contained in various FAR clauses. Nevertheless, it is prudent for all contractors and their business partners to be cognizant of the baseline ethical and conduct commitments they are making when they enter into government contracts and subcontracts. Those commitments are described in this section.

A. The FAR Clause on Business Ethics and Conduct

Contracts with a value expected to exceed $5.5 million (and with a performance period of 120 days or more) contain FAR 52.203-13, the "Contractor Code of Business Ethics and Conduct" clause. This clause commits the prime contractor to have a written code of conduct made available to employees, to exercise due diligence to prevent and detect criminal conduct, to promote an organizational culture that encourages ethical conduct and compliance, and to timely disclose credible evidence of certain wrongdoing in connection with their government contracts and subcontracts (specifically, violations of Federal criminal law involving fraud, conflict of interest, bribery or gratuities, or violations of the civil False Claims Act). Additional FAR 52.203-13 commitments (which apply unless the contract is for commercial items or with a small business) include a business ethics awareness and compliance program and an internal control system, which are described in more detail in the clause.

Other FAR clauses obligate the contractor to disclose evidence of significant overpayments on the prime contract (52.212-4(i)(5), 52.232-25(d), 52.232-26(c), 52.232-27(l)) and to report possible violations of the Anti-Kickback Act when the contractor "has reasonable grounds to believe that [such a] violation may have occurred." FAR 2.203-7(c)(2). Violations of the Anti-Kickback Act occur when a prime contractor or subcontractor, or their respective employees, make or accept payments or other things of value from each other "to improperly obtain or reward favorable treatment in connection with a prime contract or a subcontract." 41 U.S.C. § 8701(1).

B. Application to Supply Chain

The above-described FAR commitments present complex legal and practical issues for the *internal* operations of prime contractor and subcontractors that are beyond the scope of this Toolkit. We address here the additional challenges that are involved in *external* relations between a prime contractor and subcontractor.

FAR 52.203-13 expressly addresses prime-sub relations in at least three respects: (1) The disclosure commitment encompasses situations where the prime contractor has credible evidence of wrongdoing by a subcontractor (broadly defined as "any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor"). FAR 52.203-13(a), (b)(3)(i). (2) The business ethics awareness and compliance program commitment includes training for agents and subcontractors "as appropriate." FAR 52.203-13(c)(1)(ii). (3) The substance of the entire clause is to be included (i.e., flowed down) in subcontracts that meet the size and duration thresholds that trigger its applicability to prime contracts. FAR

52.203-13(d) In addition, the preamble to the Federal Register notice finalizing the clause suggested that prime contractors should engage in "reasonable efforts" to avoid subcontracting with companies that have engaged in illegal acts, and that "[v]erification of the existence of [a conduct code and compliance program] can be part of the standard oversight that a contractor exercises over its subcontractors." 3 Fed. Reg. 67084 (Nov. 12, 2008).

Prime contractors should consider undertaking various measures during subcontractor selection, when they may have the most leverage – e.g., where the subcontractor is in competition with other potential subcontractors to join the team. Information about the subcontractor's compliance program and track record can be obtained and reviewed. Clauses can be negotiated that require certifications, notifications and ongoing access to information. Careful attention should be paid to flow downs and potential enhancements thereof, particularly in areas that present substantial legal risks such as procurement integrity and interaction with government employees.

During performance, prime contractors should consider reviewing and monitoring not only their subcontractors' technical and cost results but also their subcontractors' business ethics and conduct. Monitoring kickback prohibitions can be particularly difficult because (a) whether a payment or gift violates the statute depends on whether it is made for the purposes cited in the statute, which are ill-defined and subjective; and (b) relationships between a prime contractor and its subcontractors often encompass not only government business (where kickbacks are illegal) but also commercial business (where they may not be).

If an issue arises that may be subject to disclosure, assessing whether there is "credible evidence" or "reasonable grounds to believe" wrongdoing has occurred will be more complicated insofar as relevant information is in the subcontractor's possession. Prime contractors will not have direct authority over the relevant subcontractor employees or information, and the subcontractor may be reluctant to disclose potential wrongdoing to a separate company that may be a competitor in other pursuits. Even when the subcontractor fully cooperates with the prime contractor's inquiry, there will be additional complexities in regard to the application of attorney-client and work product protection to the results of the inquiry. (Some of these complexities are described and analyzed in our alerts, including Steptoe's September 2, 2015 Alert and earlier Alerts addressing the *Barko* litigation.) In addition, a prime contractor might face litigation exposure if its communications to the Government were to contain derogatory misinformation about the subcontractor. Moreover, once government investigators are alerted to potential wrongdoing by a subcontractor, they may request the prime contractor to avoid alerting the subcontractor to the ongoing inquiry. This may excuse the prime contractor from delving further into its subcontractor's business, but it will also impede the prime contractor's ability to fulfill its commitments under FAR 52.203-13.

In short, prime contractors should not turn a blind eye to their subcontractors' business ethics and conduct. Even before potential subcontractors are identified and ultimately engaged, a prime contractor should give careful thought and preparation to how it will evaluate business ethics in its supply chain.

C. 2016 Update

1. Regulatory Developments

There have been two final rules that increase prime contractor policing requirements.

a. "Fair Pay and Safe Workplaces"

The FAR Council published a final rule on August 25, 2016, to implement Executive Order (EO) 13673 addressing "Fair Pay and Safe Workplaces." The final rule was accompanied by additional FAR and Department of Labor (DoL) guidance. *See* Federal Acquisition Regulation, Fair Pay and Safe Workplaces, 81 Fed. Reg. 58,562 (Aug. 25, 2016); Guidance for Executive Order 13673, "Fair Pay and Safe Workplaces," Final Guidance, 81 Fed. Reg. 58,653 (Aug. 25, 2016). The stated purpose of EO 13673 is to improve contractor compliance with labor laws, increase efficiency, and "cost savings" in Federal contracting.

The EO requires that prospective and existing contractors on covered contracts (contracts with an estimated value exceeding $500,000 and subcontracts over this value, other than subcontracts for commercially available off-the-shelf (COTS) items), disclose decisions regarding violations of certain labor laws. The EO also creates a new position, agency labor compliance advisors (ALCAs), to work with contracting officers. The final rule also makes labor compliance a factor in the determination of contractor responsibility. In making such determinations, contracting officers must now consult with ALCAs and consider the decisions (including any mitigating factors and remedial measures) as part of the contracting officer's decision to award or extend a contract.

The EO also creates new paycheck transparency directives, requiring that workers on covered contracts are given certain information each pay period to verify the accuracy of what they are paid and that employers inform individuals who are being treated as independent contractors. Finally, the EO limits the use of pre-dispute arbitration clauses in employment agreements on covered federal contracts.

The final rule provides a phase-in process for the disclosure of labor law decisions to give affected parties time to familiarize themselves with the rule, set up internal protocols, and create or modify internal databases to track labor law decisions in a more readily retrievable manner. Thus, when the rule takes effect, the disclosure reporting period will be limited to one year; it will gradually increase to three years by October 25, 2018. Moreover, during the first six months that the rule is effective (i.e., until April 24, 2017), the disclosure requirement will apply only to solicitations for contracts valued at $50 million or more.

Subcontractor disclosure is also being phased in under a delayed effective date. Subcontractors will be required to report labor law decisions if they are seeking to perform covered work under Federal contracts awarded pursuant to solicitations issued one year after the rule takes effect – i.e., on or after October 25, 2017. Subcontractor disclosures are to be made directly to the DOL, not to the prime contractor. However, subcontractors are also to make a statement to the prime contractor regarding DoL's response to the subcontractor's disclosure when the subcontractor is not in agreement with, or has concerns with, DoL's assessment. The

prime contractor is to consider the DoL response to subcontractor disclosures in evaluating the integrity and business ethics of subcontractors.

The final rule also requires prospective prime contractors to publicly disclose certain information about covered violations such as: the law violated, the case identification number, the date of the decision finding a violation, and the name of the body that made the decision. This disclosure requirement applies to civil judgments and administrative merits determinations, including judgments and determinations that are not final or are still subject to review, as well to arbitral awards. However, the final rule does not compel public disclosure of additional documents the prospective contractor deems necessary to establish its responsibility, such as documents demonstrating mitigating factors, remedial measures, and other steps taken to achieve compliance with labor laws, unless the contractor determines it wants this information made public.

The final rule applies to decisions concerning violations of a broad range of federal labor laws, including, among others: the Fair Labor Standards Act, the Occupational Safety and Health Act, the National Labor Relations Act, the Davis-Bacon Act, the Service Contract Act, the Family and Medical Leave Act, the Americans with Disabilities Act, the Age Discrimination in Employment Act, and violations of state plans approved by OSHA. Disclosure and consideration of decisions concerning other equivalent state law violations may be added in the future.

Finally, the Federal Register announcement indicates that the final rule applies to the legal entity whose name and address is entered on the bid/offer and would be legally responsible for performance of the contract, unless a specific FAR provision (e.g., FAR 52.209–5 Certification Regarding Responsibility Matters) requires additional information. The legal entity that is the offeror does not include a parent corporation, a subsidiary corporation, or other affiliates. A corporate division is part of the corporation.

On October 25, 2016, the date on which the rule's reporting and disclosure obligations were to become effective, a federal district court in Texas entered a nationwide preliminary injunction stopping the Government from moving forward with the reporting and disclosure of the Fair Pay and Safe Workplaces final rule, as well as the rule's prohibition on mandatory pre-dispute arbitration agreements covering Title VII or sexual assault/harassment claims. However, the rule's paycheck transparency and independent contractor notice requirements were not enjoined. Those provisions will become effective on January 1, 2017, for covered contracts of more than $500,000 (other than commercially available off-the-shelf items). Following the court's order, the Office of Federal Procurement Policy issued a memorandum that instructs agencies to take required steps to comply with the court order. The memorandum also states that agencies are to continue their evaluations of offerors, including responsibility determinations. However, this rule has been the subject of controversy, and its status going forward may be affected by the upcoming change in Administration.

b. "Establishing Paid Sick Leave for Federal Contractors"

DoL published a final rule on September 30, 2016, on "Establishing Paid Sick Leave for Federal Contractors," which became effective on November 29, 2016. *See* 81 Fed. Reg. 67,598

(codified at 29 C.F.R. § 13). It implements Executive Order 13706, which requires certain parties that contract with the federal government to provide their employees with up to seven days (56 hours) of paid sick leave annually, including paid leave allowing for family care. On December 16, 2016, the FAR Councils followed suit by issuing interim FAR provisions and clauses that are basically consistent with DOL's regulations with respect to procurement contracts. 81 Fed. Reg. 91627. The FAR interim rule is effective as of January 1, 2017 and thus applies to certain solicitations issued on or after that date (to include resulting contracts). DoL also issued a "Fact Sheet" with additional explanatory material.

These regulations generally incorporates existing definitions, procedures and enforcement processes under other authorities, to include the Fair Labor Standards Act, the Service Contract Act, the Davis-Bacon Act, the Family and Medical Leave Act, the Violence Against Women Act, and Executive Order 13658 (Establishing a Minimum Wage for Contractors).

The final regulations apply only to the specific categories of contracts listed below and, with certain limited exceptions, only to contracts awarded pursuant to solicitations issued on or after January 1, 2017 and that are performed "within the United States":

- Procurement contracts for construction covered by the Davis-Bacon Act (DBA)
- Contracts for services covered by the Service Contract Act (SCA);
- Contracts for concessions, including any concessions contract excluded from coverage under the SCA by the DoL regulations at 29 CFR 4.133(b);
- Contracts in connection with federal property or lands and contracts related to offering services for federal employees, their dependents, or the general public; and
- Certain contracts with the US Postal Service.

The final regulations do not apply to grants, to contracts with or grants to Native American Tribes under the Indian Self-Determination and Education Assistance Act (Public Law 93–638), or contracts that are subject only to the Davis-Bacon and related acts. According to the comments accompanying DoL's final rule, the Executive Order also does not apply to the following:

(i) prime contracts for the "manufacturing or furnishing of materials, supplies, articles, or equipment," and similar subcontracts, including subcontracts for materials, supplies, articles, or equipment for use on a covered contract; and

(ii) a significant portion of commercial items contracts, including "commercial supply contracts subject to the Walsh-Healey Public Contracts Act."

There is no dollar value threshold for application of these requirements to subcontracts awarded under covered prime contracts (i.e., those covered by the SCA, DBA, or Fair Labor Standards Act), or the other categories of contracts listed above.

The regulatory scheme permits a contractor to satisfy its obligations by providing paid sick time that fulfills the requirements of a state or local law, provided that the paid sick time is accrued and may be used in a manner that meets or exceeds all of the requirements of the final rule. Where the requirements of an applicable state or local law differ from the final federal rules, contractors are directed to "comply with the requirement that is more generous to employees."

Significantly, the final rules make prime contractors and any upper-tier subcontractors responsible for the compliance by any subcontractor or lower-tier subcontractor – regardless of whether the contract clause was included in the subcontract.

DoL is responsible for enforcement of these regulations, including the investigation of potential violations. DoL's rules include procedures for resolution of disputes concerning a contractor's compliance, but neither Executive Order 13706 nor the final rule creates or changes any rights under the Contract Disputes Act or creates any private right of action. The FAR's interim rules also provide that "[d]isputes related to the application of E.O. 13706 . . . shall not be subject to the general disputes clause" of the contracts at issue. Of course, contractors may have other remedies, including judicial review of final decisions by the Secretary of Labor in accordance with the Administrative Procedure Act. Finally, DoL's dispute resolution procedures also may not limit or preclude other remedies available to the Government, such as a civil action under the False Claims Act, 31 U.S.C. § 3730, or criminal prosecution under 18 U.S.C. § 1001.

2. Case Law

During the past year several prosecutions, settlements, and pleas have emphasized the focus on kickback enforcement and supply chain risks to contractors. This reinforces the importance of active due diligence by the prime – potentially including "hands on" involvement – when suppliers are not familiar with the government contracting environment and compliance responsibilities.

a. *Guilty Pleas in Kickback Case*

The fall of 2015 saw guilty pleas in the Southern District of Florida from a former employee of a federal contractor and from a subcontractor for violating the Anti-Kickback Act.

In that case, as reported by the Department of Justice, the contractor employee received more than 50 wire transfers from the subcontractor, totaling almost $2 million, in return for a promise to ensure additional business and not to engage in behavior that would adversely affect the subcontractor. The funds were directed to shell bank accounts that filed false tax returns. Both the contractor employee and the subcontractor received fines and prison terms (four years and one year, respectively), and were debarred from federal contracting. Press Release, US Dep't of Justice, Federal Government Contractor Pleads Guilty to Accepting Kickbacks and Tax Evasion (Oct. 23, 2015).

b. Charges in Kickback Scheme Involving Aerospace Firm

In April 2015, the US Attorney's Office for the Central District of California announced that it had charged seven employees of a subcontractor in a kickback scheme involving $750K in

payments to the prime contractor's procurement official at an aerospace company. The announcement alleged that a subcontractor, which provided tooling parts used to manufacture satellites, had paid kickbacks to the prime's procurement officer in exchange for confidential information that gave the subcontractor a competitive advantage in bidding for subcontract awards. The US Government alleged that, as a result of this scheme, the subcontractor had received approximately $4.5 million in purchase orders and, even after the prime stopped doing business with the subcontractor due to performance issues, the subcontractor continued to do business with the prime through a "front" company.

At least five of the seven defendants pled guilty, including the prime's procurement officer who received the kickbacks. All were suspended from federal contracting. Press Release, US Dep't of Justice, 7 Charged In Scheme To Pay Hundreds Of Thousands Of Dollars In Kickbacks . . . To Secure Contracts Related To Satellites (Apr. 2, 2015).

Lesson: This kickback scheme was brought to the Government's attention by the prime contractor, after conducting an internal investigation prompted by a hotline report. By maintaining an effective compliance program, the prime contractor was able to limit the consequences to the one "bad apple" in its employ.

c. *Prime Contractor Found Vicariously Liable under Anti-Kickback Act*

On October 15, 2015, the District Court for the Eastern District of Texas found a prime contractor vicariously liable under the Anti-Kickback Act for the actions of two former employees. The prime contractor was assessed a civil penalty of $108,342, reflecting the amount of the thirty-three kickbacks charged ($4,671, doubled), which the court believed was understated, plus thirty-three penalties of $3,000 each. The prime contractor has appealed this penalty to the Fifth Circuit.

Although one of the former employees had pled guilty to receiving kickbacks from two subcontractors, the prime contractor contended that the meals, entertainment, and golf outings at issue were "relationship-building" rather than kickbacks, and that the former employees were not in a position to influence subcontract awards. The prosecutors, and ultimately the court, felt otherwise. (The subcontractors had previously paid fines of hundreds of thousands of dollars, without admitting liability.)

The District Court found that the prime contractor placed the former employees in positions responsible for awarding and overseeing millions of dollars in subcontracts that would be charged to the federal government but provided little oversight, allowing their conduct to go unchecked for more than two years. "Had [the prime contractor], through training, supervision, and guidance, impressed on its employees a culture of integrity and been diligent in monitoring the . . . subcontract, it is unlikely that so many could have so openly and for so long accepted these kickbacks without concern for their jobs, or any thought that someone would blow the whistle." Press Release, US Dep't of Justice, dated Oct. 16, 2016.

Lesson: Though the decision could yet be reversed on appeal, this case highlights that the company is often "on the hook" for the bad acts of its employees and, as a result, the

importance of an effective compliance program and training in the subcontract administration area.

d. *Settlement of Prime and Subcontractor Civil False Claims Act Allegations*

In November 2015, a subcontractor agreed to pay $11.4 million and the prime contractor agreed to pay $1.35 million to resolve (without an admission of liability) allegations that they used individuals without security clearances on a DISA contract.

According to the Department of Justice announcement, the subcontractor allegedly used employees without security clearances to perform work that the contract required be done with cleared individuals, which led to the prime contractor filing invoices that the Government considered to be false claims. The lawsuit was originally filed by a qui tam whistleblower, who received more than $2 million as his share of the recovery.

At the time of the settlement, the prime contractor made a public statement that it "believes it is as much a victim of [the subcontractor's] conduct as is our DISA customer and agreed to settle this case because the litigation costs outweigh those of the settlement." Press Release, dated Nov. 2, 2015.

Lesson: Prime contractors may be exposed to some of the same consequences as their subcontractors and cannot afford to take a "hands-off" approach to the performance of their subcontractors.

V. Teaming and Collaborative Arrangements

Teaming and other collaborative arrangements, such as joint ventures, can offer a working arrangement that extends through both the pursuit and performance of a government contract. A teaming relationship involves collaboration prior to awarding a subcontract, rather than merely issuing a purchase order only after the prime contractor has been selected for contract award. The past performance, experience, and personnel of the teaming partner may be essential during the pursuit stage and in the proposal in order to satisfy the requirements of the RFP. Teaming arrangements are popular because these arrangements can effectively pool the strengths of companies and combine complementary skills, as well as develop competitive strategies in order to address fierce competition for contracts.

Forming a team is often necessary to enter a new marketplace or win a large program requiring the integration of different skills. The arrangement may be formed for a specific, limited purpose or, when appropriate, for a longer period spanning several transactions. In all circumstances, care must be taken to avoid antitrust problems.

Due to the frequency of team formation, some may mistakenly believe that the process of forming a team with another company, perhaps one that is also a competitor, is easy and without significant risk. That is not the case. The formation of a team presents both opportunities and challenges. Approach such a "marriage of convenience" with caution. Companies in a team arrangement may possess legal rights and expectations which, if unfulfilled, can give rise to disputes, claims and legal actions.

A. Why Team?

When deciding whether to team, the first question to ask is whether a subcontract or purchase order will suffice. In many cases, that is all that is required to work together. The frequency of teaming today, however, indicates that companies often desire a stronger and longer bond and commitment than is offered by a post-award subcontract. Obtaining a key subcontractor's support through the bid and proposal effort may require the prime contractor to make a commitment to award a subcontract, something that a teaming agreement can do. An opportunity may require the combination of specific complementary capabilities that may be beyond the capabilities held by a single company. To be responsive to marketplace requirements, such as a Request for Proposal for a large system, it is common for companies to team in order to obtain and offer the full range of required capabilities.

FAR Subpart 9.6 supports contractor team arrangements when the teaming partners complement each other's capabilities and offer the Government the best combination of performance, cost and delivery. It requires teaming arrangements to be identified and disclosed, however, and maintains the Government's rights to hold the prime contractor fully responsible for contract performance, regardless of any team arrangement between the prime contractor and its subcontractors.

B. What Are the Benefits of Forming a Team Arrangement?

The most important benefit is the ability to obtain complementary capabilities required by the marketplace. Other benefits include sharing development, performance, or financial risks, gaining a competitive advantage through a teammate's past performance, or learning from an experienced company, such as in a mentor-protégé program.

A team arrangement may limit certain options by virtue of the legal obligations that follow the formation of such a relationship. For example, the team arrangement may assure a source for certain work, but may inhibit a change in management desires to "make" rather than "buy." Teaming with a company possessing the same core competencies may signal the need to examine the possibility of anticompetitive issues. The antitrust laws should be considered when competitors form a team arrangement – in fact, FAR Subpart 9.6 forbids team arrangements that are "in violation of antitrust statutes." And FAR 3.303(c)(7) specifically recognizes, as an antitrust flag, "[t]he filing of a joint bid by two or more competitors when at least one of the competitors has sufficient technical capability and productive capacity for contract performance." In fact, a teaming arrangement can be challenged on antitrust grounds even if the agency had advance knowledge that the contractors intended to form a team arrangement, or even if the agency encouraged the arrangement.

For a teaming arrangement to be successful, it should be accompanied by an agreement as to how the workshare will be divided if the team is awarded the contract, because the parties' negotiating leverage may change at contract award. A team member may be vital to winning the award but replaceable thereafter, allowing the prime contractor to leave the teaming partner at the altar when it comes time to negotiate the subcontract – or so the would-be subcontractor might fear. Conversely, if a teaming partner is critical to performing the contract successfully, it may move into the driver's seat after award – or at least that may be the prime contractor's fear.

Even though a typical teaming agreement will not include many of the provisions that must be contained in a subcontract – indeed, it may not even contain sufficient material terms to be enforceable in court – it may be important for the teaming agreement to contain certain provisions that are critical to the relationship, such as intellectual property rights, limitations on liability, the extent of exclusivity, and no-hire commitments.

C. Due Diligence Is a Necessary Step

Relevant information must be obtained about a company prior to forming a team. Even a simple arms-length purchase order negotiation with a supplier will benefit from some basic due diligence. In a team, where the parties will be closely working together, due diligence is a vital element in the process. A prime contractor that is forming a team could be considering an entity, maybe even a competitor in other areas, with which it has not worked closely in the past. Due diligence is especially important in the formation of a joint venture, because each partner may face joint and several liability for the actions of its other partners.

Due diligence means conducting the type of inquiry that a reasonably prudent company would conduct before entering into a relationship with legal obligations. A due diligence inquiry can reveal red flags, and should provide important insight into terms and conditions that will

need to be negotiated in the teaming agreement and subsequent subcontract in order to protect the prime contractor's interests. The teaming agreement should not be limited to a form with standard boilerplate clauses; it should include tailored provisions resulting from the due diligence inquiry.

An important aspect of due diligence is the identification of any issues that could reduce the team's chances of being selected for award. For example, legal problems and ethical lapses or other issues that could raise responsibility concerns or potentially lead to suspension or debarment would make a company a risky teaming partner, and could prevent the team's selection. Likewise, performance problems on prior contracts, contract terminations, or claims against the potential partner would indicate unfavorable past performance. The importance of past performance as a major source selection factor, which often includes past performance of teaming partners, makes such a review very important.

Organizational conflict of interest (OCI) issues and personal conflict of interest (PCI) issues also should be considered and evaluated. For example, an OCI may arise if a teaming partner (i) has (or had) access to non-public information related to the procurement; (ii) had input into the statement of work or specifications; (iii) performed Systems Engineering and Technical Assistance in the program; or (iv) has business interests that could be affected by performance of the contract. The inclusion of a team member with an OCI problem, or with employees who may pose a PCI problem, could lead to a disqualification of the team unless the OCI or PCI can be mitigated.

Ensuring that your partner will provide the level of resources and management commitment necessary to assure success should not be merely an issue for contract draftsmanship and possible legal recourse. It needs to be examined and questioned during the due diligence inquiry.

D. What about Exclusivity?

A question that teammates must consider is whether the arrangement should be exclusive, meaning that each teammate will not be allowed to join a different team in competition for the same contract award. When companies collaborate as a team and prepare a proposal in response to an RFP, they typically share proprietary information, including team strategies. An arrangement that is not exclusive tends to inhibit the free flow of information. When a teaming partner plays on multiple teams, it must generally erect firewalls, isolate proposal writers, and exclude certain team members from certain strategy sessions. These alternatives are burdensome at best, and may not be feasible, particularly when small businesses with limited staffs are involved.

The agencies charged with policing anticompetitive behaviors, including the Federal Trade Commission (FTC) and the US Department of Justice (DOJ), have noted the benefits of collaborative efforts between companies. They recognize that, to compete in today's marketplace, companies that are competitors in some situations might need to collaborate as teammates in other situations. Nonetheless, increasing consolidation in the defense industry caused the FTC and DOJ to issue a joint statement on April 12, 2016, to explain their standard of antitrust review of proposed transactions within the industry. In this statement, they re-pledged

their vigilance, in cooperation with the Department of Defense (DoD), to ensure that consolidation does not make it harder for DoD to acquire needed equipment and services at competitive prices in current and future procurements.

The joint DOJ-FTC statement also refers to potential anti-competitive effects of team arrangements and other joint business arrangements. Concern over the potential anti-competitive effects of team arrangements is not new. This attention has grown, however, because competition for large procurements has often become team versus team rather than company versus company. In many cases, the teaming approach was consistent with the needs of those specific procurements, which required the combination of a variety of complementary capabilities to satisfy a broad range of requirements.

That said, exclusive arrangements may raise questions of possible anticompetitive impact. The joint statement is a reminder that contractors need to consider the potential effects on competition when they consider exclusive team arrangements in the pursuit of government contracts – prior to formalizing a teaming relationship. Some agencies also have supplemental FAR clauses that either require disclosure of exclusive arrangements or expressly prohibit them. Therefore, it is important to carefully review the RFP and incorporated FAR clauses to ensure that any proposed exclusivity is consistent with the RFP's terms.

E. Is a Particular Teaming Agreement Enforceable?

An issue that accompanies the formation of teaming agreements is whether the agreement is an enforceable agreement or merely an unenforceable "agreement to agree." The vast majority of disputes between team members are resolved through negotiation. In fact, many teaming agreements seek to avoid court action and expressly provide procedures to resolve disputes in the context of a more cooperative arrangement. Such agreements may include internal escalation procedures and the use of alternative dispute resolution mechanisms such as mediation or arbitration.

Despite the frequency of negotiated settlements, however, some disputes do proceed into the court system. A number of judicial decisions have addressed whether the court should enforce a particular teaming agreement. In a 1964 "team arrangement" decision, a court found that "team membership" on a team seeking the award of an Air Force contract meant more than providing one company the opportunity to bid on a subcontract – it meant that if the prime contractor received the prime contract, the team member was to receive a subcontract (subject to Air Force approval). Subsequent case law, however, indicates that without a clear intent to be bound and sufficient agreement on material terms of the subcontract, a teaming agreement may be treated as an unenforceable "agreement to agree."

The reality is that under the time pressures of competition, it may not be possible to negotiate a definite subcontract that would ensure enforceability. Moreover, there may be times when one or the other party prefers that the teaming arrangement not be enforceable in court. The bottom line is that parties to a team arrangement should not depend on a court to hold the other party's feet to the fire; they should come together because – and only because—they have mutual and strong desires to win the award and work together.

F. Recent Cases Involving Enforceability of Teaming Agreements

- ***A-T Solutions Inc. v. R3 Strategic Support Group Inc.*, Civ. No. 3:16-cv-00007 (E.D. Va. 2016)**

In this case, A-T Solutions, as prime contractor, and R3 Strategic Support Group, as subcontractor, entered into a teaming agreement to pursue the Combined Explosive Exploitation Cell (CEXC) program. The teaming agreement provided that neither party would "participate in any manner or undertake any efforts in support of any other teaming efforts that are competitive to this Teaming Agreement." After executing the teaming agreement the parties commenced their CEXC collaboration, but two months later, the Government cancelled the CEXC solicitation "to allow for a reassessment of the mission requirements and revisions."

Five months later, however, the Government proceeded with a new procurement based on a revised CEXC solicitation. R3, the original subcontractor, took the position that the earlier Teaming Agreement was no longer valid, having been terminated by the cancellation of the solicitation. A-T Solutions, on the other hand, contended that the teaming agreement remained in effect for this procurement. It then went to federal court seeking to prevent its former teammate from competing against it and potentially making use of A-T Solutions' trade secrets. A-T Solutions even went so far as asking for a preliminary injunction compelling R3 to team with A-T Solutions for the CEXC program.

In response, R3 claimed that Virginia precedent made its teaming agreement with A-T Solutions an unenforceable "agreement to agree," arguing that its teaming agreement was "indistinguishable" from other teaming agreements held to be unenforceable under Virginia law. Ruling from the bench, the Federal District Judge agreed that the teaming agreement was unenforceable and denied A-T Solutions' motion for an injunction. As a result of this ruling, A-T Solutions voluntarily dismissed its lawsuit.

In addition to demonstrating the risks to teaming members about unenforceable "agreements to agree," this case also highlights the importance of clearly defining the parameters of the relationship, including when the relationship automatically terminates.

- ***Navar, Inc. v. Federal Business Council*, 784 S.E. 2d 296 (Va. 2016)**

In *Navar*, the Virginia Supreme Court put an exclamation point on the risk under Virginia law that teaming agreements lacking specificity will be treated as mere "agreements to agree." This case involved a contract for event planning services solicited by the United States Defense Threat Reduction Agency (DTRA). Because the RFP required that the awardee be an Alaska Native Corporation (ANC), neither of the plaintiffs in Navar, the Federal Business Council (FBC) and Worldwide Solutions, Inc. (WSI), could bid on the contract as a prime contractor. Instead, they identified Navar, Inc., a qualified ANC, as the proposed prime contractor. The parties then executed a non-disclosure agreement (NDA), attended a meeting with DTRA to discuss their proposal, and executed a teaming agreement. The teaming agreement provided that, if Navar won the DTRA contract, it would negotiate in good faith with FBC and WSI and, "upon arriving at prices, terms and conditions acceptable to the parties," would enter into subcontracts with them. That is common teaming agreement language.

DTRA indeed awarded a $55 million contract to Navar, and Navar commenced negotiations with FBC and WSI. Negotiations, however, broke down and no subcontracts were awarded. FBC and WSI then filed a lawsuit against Navar based on the failure to award subcontracts to them, seeking damages (including lost profits) for breach of the parties' teaming agreement and NDA, and for alleged violations of the Virginia Trade Secrets Act.

The result was a three-act play.

The plaintiffs won the first act – the jury found in favor of the two aggrieved teammates, awarded each of them $500,000 for breach of the teaming agreement, and awarded one teammate an additional $250,000 for breach of the NDA. These judgments, however, were fated not to stand.

The second act was a split decision. In response to Navar's motion for reconsideration, the trial judge "split the baby" – on the breach of contract verdict, he disregarded the jury's finding and entered judgment for Navar (notwithstanding the jury verdict) on the ground that the teaming agreement was unenforceable as a matter of law. But he denied Navar's motion to reconsider the jury's finding that Navar was liable for breach of the NDA and for violation of the Virginia Trade Secrets Act.

The third and decisive act was a total victory for Navar. The Virginia Supreme Court affirmed the trial court's decision finding the teaming agreement unenforceable as a matter of law, but reversed the jury's and trial court's findings of Navar's liability based on the alleged breach of the NDA and violation of the Virginia Trade Secrets Act. The Virginia Supreme Court found that Navar had no liability to its teaming members.

What is the takeaway? Yet again, the Virginia courts have found that a teaming agreement was an unenforceable "agreement to agree."

VI. Counterfeit Parts

Counterfeit parts in the supply chain represent a significant threat to end users and are a major concern of government buyers. The importance of this issue resulted in a requirement for contractors supplying the Department of Defense (DoD) with electronics or items that contain electronic parts to implement procedures adequate for detecting, and avoiding the use or inclusion of counterfeit parts, where those parts are provided under contracts subject to full or modified coverage under the Cost Accounting Standards (CAS). The current rule, although limited to DoD, provides a model for a system to detect, monitor, and eliminate counterfeit parts, and an expanded rule is anticipated that will address the risk of counterfeit parts for all government agencies.

A. The Counterfeit Electronic Parts Rule

As explained by Senator Levin in a press release, the Senate Armed Services Committee investigated counterfeit electronic parts finding their way into US military defense systems, and found a flood of counterfeit electronic parts entering the defense supply chain and endangering our troops.

This investigation prompted legislative action to address counterfeit parts in the supply chain for DoD. Those mandates are found in the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012, Pub. L. 112–81, § 818, 125 Stat. 1298, and FY 2013, Pub. L. 112-239, § 833, 126 Stat. 1632. Section 818 of the FY 2012 NDAA requires the Secretary of Defense to assess DoD's "acquisition policies and systems for the detection and avoidance of counterfeit electronic parts." Section 833 does not allow the reimbursement of costs associated with counterfeit electronic parts or with corrective actions to remedy the use or inclusion of such parts, except where a contractor implements a system for detecting and avoiding counterfeit electronic parts.

As a result of this legislative action, DoD issued a final rule in May 2014 under DoD Federal Acquisition Regulation Supplement (DFARS) requiring that contractors establish and maintain a risk-based electronic system to monitor, detect, and eliminate counterfeit parts. See DFARS Subpart 246.870. Noncompliance threatens the contractor's ability to conduct business with the Government.

B. Important Definitions

The DFARS rule applies to counterfeit electronic parts, suspect electronic parts, and obsolete electronic parts, including any embedded software or firmware. The definitions in the rule at DFARS 202.101 are important and are set forth below:

> A "counterfeit electronic part" is "an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer."

An "unlawful or unauthorized substitution" is defined to include used electronic parts represented as new or otherwise false indications of "grade, serial number, lot number, date code, or performance characteristics."

A "suspect counterfeit electronic part" is one "for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic." The "credible evidence" standard is not defined in the rule.

An "obsolete electronic part" is one "no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer." The rule's preamble explains that guidance concerning supply chain processes to mitigate risks inherent with obsolete parts is beyond the scope of the final rule.

C. The Rule's Reach

The rule is an effort to formalize the efforts required to identify and address counterfeit electronic parts in government contractor's supply chains. DFARS clause 252.246-7007 provides an outline for an adequate counterfeit part detection and avoidance system. The contractor is required to follow this only if they are providing DoD with electronic parts, end items, components, parts or assemblies containing electronic parts, and services. The DFARS clause applies to contractors subject to full or modified coverage under CAS. It also applies to subcontractors under CAS-covered prime contractors, regardless of the subcontractor's CAS or size status.

The final rule also is applicable to commercial items and commercial-off-the-shelf (COTS) items if those items are being supplied to a CAS-covered contractor. This means that prime contractors and higher tier subcontractors should pay close attention to (and may have to police) the commercial suppliers and vendors in their supply chains.

D. Mandates for a Supply Chain Counterfeit Electronic Part Detection and Avoidance System

Covered contractors must establish and maintain an acceptable counterfeit electronic part detection and avoidance system. The system must include risk-based policies and procedures that address, at a minimum, the following twelve attributes:

1. Training is essential and the first area mentioned; however, the rule leaves to contractors the ability to develop appropriate training based upon their needs.

2. The rule states that selection of tests and inspections of electronic parts by the contractor "shall be based on minimizing risk to the Government."

3. The rule's preamble states that the contractor must report to the contracting officer and to the Government-Industry Data Exchange Program (GIDEP) when the contractor "becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts . . . contains counterfeit electronic parts or suspect counterfeit electronic parts."

4. The rule requires traceability of the electronic part to the original manufacturer, but does not require that any particular procedure be used. It does require that the procedure chosen must include "certification and traceability documentation developed by manufacturers in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and where, available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers."

5. Electronic parts must come from the original manufacturers or authorized sources. If not available from these sources, suppliers that "meet applicable counterfeit detection and avoidance system criteria" are acceptable.

6. In addition to reporting to the Contracting Officer and to GIDEP, contractors also must retain the counterfeit or suspect counterfeit parts until "until such time that the parts are determined to be authentic."

7. Contractors are to use a risk-based methodology to "rapidly determine if a suspect counterfeit part is, in fact, counterfeit."

8. Contractors must design, operate, and maintain systems to detect and avoid counterfeit and suspect electronic parts, but "may elect to use current Government- or industry- recognized standards to meet this requirement."

9. The prime contractor must flow down counterfeit detection and avoidance requirements, including system criteria to its subcontractors and suppliers at all levels. This emphasizes the requirement to police the entire supply chain, which could span the globe and could include commercial subcontractors. Even non-CAS suppliers and subcontractors are implicated if they are contracting with a CAS-covered prime.

10. Contractors must have processes to keep informed of counterfeiting issues and use current information and trends to continuously upgrade internal procedures.

11. Contractors are required to continuously review GIDEP and other credible reports of counterfeit parts that could impact their supply chains.

12. Contractors must control obsolete electronic parts in order to maximize the availability and use of the authentic parts during the products life cycle.

E. Government Review and Remedies

The Government reviews compliance with the counterfeit parts rule through the Contractor Purchasing System Review (CPSR) conducted by the Defense Contract Management Agency (DCMA). The rule's preamble states that CPSRs will examine the contractor's policies and procedures for the detection and avoidance of counterfeit electronic parts. If DCMA identifies a "significant deficiency" – i.e., a shortcoming in the system that materially affects the

ability of DoD to rely upon the purchasing system – DCMA can decide to disapprove the contractor's purchasing system or to withhold payment.

A section of the FAR cost principles at DFARS 231.205-71 addresses costs associated with remedying counterfeit electronic parts. Costs incurred in remedying the use of counterfeit or suspect counterfeit electronic parts are expressly unallowable under the rule, unless the contractor's system for detecting and avoiding counterfeit electronic parts has been reviewed and approved or the counterfeit or suspect counterfeit electronic parts are government-furnished, and the contractor provides notice within 60 days of becoming aware of the counterfeit or suspect counterfeit electronic part.

F. Anticipated Broader Rule

The current DFARS rule does not reach all government contractors. However, it represents the type of system that the government expects to see and it provides a model for contractors. The current requirement for a counterfeit electronic parts detection and avoidance system is applicable to CAS-covered prime contracts, but can reach non-CAS companies through the flow down requirement to all companies in a prime contractor's supply chain. The flow down requirement can impact subcontracts for commercial items and subcontracts with small businesses.

The current rule is limited to the DoD, but a broader rule is anticipated. The Federal Acquisition Regulatory Council has issued a proposed rule that would expand the coverage of the requirements for an anti-counterfeiting system beyond DoD and would include non-electronic parts. (FAR Case 2013-002, Expanded Reporting of Nonconforming Supplies). This proposed rule remains under consideration.

G. 2016 Update

1. Regulatory Developments

On March 25, 2016, DoD issued a proposed DFARS cost allowability rule (DFARS Case 2016-D010) that makes specified costs allowable when associated with the discovery and the correction of counterfeit or suspect counterfeit electronic parts. This proposed rule implements a section of the NDAA for FY 2016 that addresses the allowability of costs of counterfeit or suspect counterfeit electronic parts and addresses the cost of rework or corrective action that may be required to remedy the use or inclusion of those parts. It is intended to consider the financial burden resulting from detecting, monitoring, and remedying counterfeit or suspect counterfeit electronic parts.

Costs may be allowable if three conditions are met:

- The counterfeit or suspect counterfeit electronic parts were obtained by the contractor in accordance with the regulations described in section 818(c)(3) of the NDAA for FY 2012, as amended;

- The contractor discovers the counterfeit or suspect counterfeit electronic parts; and

- The contractor provides timely notice (i.e., within 60 days after the contractor becomes aware).

Comments accompanying the proposed rule noted that the final cost allowability rule would not be published until the final rule in DFARS case 2014-D0005, *Detection and Avoidance of Counterfeit Parts – Further Implementation*, is issued. A proposed version of that rule, which will implement section 818(c)(3) of the FY 2012 NDAA, was published on September 21, 2015. 80 Fed. Reg. 56,939 (Sept. 21, 2015).

On August 2, 2016, the DoD issued a proposed rule to amend the DFARS to implement section 885(b) of the FY 2016 NDAA. 81 Fed. Reg. 50,635 (Aug. 2, 2016). This proposed rule makes contractors and subcontractors subject to approval (as well as review and audit) by appropriate DoD officials when a contractor identifies a contractor-approved supplier of electronic parts. This proposed rule imposes only approval requirements; it does not impose any reporting, recordkeeping, or other compliance requirements. In general, a contractor may proceed with the acquisition of electronic parts from a contractor-approved supplier unless otherwise notified by DoD.

Contractors should anticipate that additional rules may result from several DFARS and FAR cases that address counterfeit parts concerns.

2. The General Services Administration (GSA) Issued an RFI for Solutions to Tackle Counterfeit IT Products in the Federal Supply Chain

In May 2016, GSA announced that it is seeking a supply chain solution as part of a pilot program aimed at helping federal procurement professionals authenticate IT and communication products in the Government's supply chain. GSA issued the RFI to gather information about the development of a supply chain solution and interface that would prevent counterfeit IT components from entering the federal supply chain, saying that "[t]he intent is to strengthen the compliance and security of the supply chain and thwart tampering, counterfeiting and grey market offerings."

The GSA's RFI asks providers to share information on their current supply chain solutions and capabilities, and note whether their solution has the ability to validate, track and authenticate commercial IT offerings in the federal government's supply chain and whether the solution can track changes of a product throughout the supply chain.

3. GAO Review: GAO-16-236, *DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk* (February 16, 2016)

The GAO conducted this study, in response to a Senate Report, because the defense supply chain is vulnerable to the risk that counterfeit parts will delay missions and endanger service members. To effectively identify and mitigate this risk, DoD has been requiring its agencies and contractors to report data on suspect counterfeit parts. The GAO report examines, among other things, (1) the use of the Government-Industry Data Exchange Program (GIDEP) to report counterfeits, (2) GIDEP's effectiveness as an early warning system, and (3) DoD's

assessment of defense contractors' systems for detecting and avoiding counterfeits. GAO analyzed data from GIDEP for fiscal years 2011 through 2015; reviewed DoD policies, procedures, and documents; and met with agency officials and contractors responsible for contracts including the new counterfeit clause.

The GAO report recommended that DoD oversee its defense agencies' reporting efforts, develop standard processes for when to report a part as suspect counterfeit, establish guidance for when to limit access to GIDEP reports, and clarify criteria for contractors in implementing their detection systems. DoD agreed with the three recommendations on GIDEP reporting but only partially agreed with the recommendation to clarify criteria, stating that it did not agree with providing specific implementation details. In response, GAO stated that it continued to believe that clarifying criteria is important, which is different from specific implementation details.

4. Enforcement

- **Citizen of China Pleads Guilty to Trafficking in Counterfeit Computer Chips**

On April 15, 2016, the United States Attorney for the District of Connecticut, announced that Daofu Zhang, 40, of Shenzen, China, had pled guilty to conspiring to sell counterfeits of sophisticated integrated circuits to a purchaser in the United States. *See United States v. Zhang*, 16-cr-00072-RNC (D. Conn. 2016); *United States v. Yan*, 16-cr-00046-RNC (D. Conn. 2016); *United States v. Zuo*, 16-cr-00040-RNC (D. Conn. 2016).

According to court documents and statements made in court, Zhang and his two co-conspirators each operated businesses in China that bought and sold electronic components, including integrated circuits ("ICs"). In the summer of 2015, Zhang's co-conspirator, Xianfeng Zuo asked the other co-conspirator, Jiang Yan, to locate and purchase several advanced ICs, made by Xilinx Corp., which had military applications, including radiation tolerance for uses in space. Yan then asked a US individual to locate the Xilinx ICs and sell them to Yan. The US individual explained that the ICs cannot be shipped outside the US without an export license, but Yan still wished to make the purchase. When the US individual expressed concern that the desired ICs would have to be stolen from military inventory, Yan allegedly proposed to supply the US source with "fake" ICs that "look the same" to replace the ones to be stolen from the military.

In November 2015, Zhang shipped from China to the US individual, two packages containing a total of eight counterfeit ICs, each bearing a counterfeit Xilinx brand label. After further discussions between Yan and the US individual, Yan, Zhang, and Zuo flew together from China to the US in early December 2015 to complete the Xilinx ICs purchase. When the three conspirators drove to the location where they planned to meet the US individual, make payment, and take custody of the Xilinx ICs, Federal agents arrested all three.

Zhang pled guilty to one count of conspiracy to traffic in counterfeit goods. Yan, pled guilty to one count of conspiracy to traffic in counterfeit goods, and one count of attempt to export integrated circuits without the required export license. Zuo pled guilty to one count of conspiracy to traffic in counterfeit goods.

- **President of Aviation Parts Company Arrested for Fraudulently Supplying Defective Airplane Parts to US Government**

On February 29, 2016, the US Attorney's Office for the Eastern District of New York announced that Paul Skiscim, President of Aerospec, Inc., was arrested on federal charges for allegedly supplying defective airplane parts to the federal government for use in its aircraft, including military aircraft. According to the complaint, Aerospec had been a supplier of airplane parts to the United States from 2003 until 2013, when the company and Skiscim were debarred after supplying the Government with defective airplane parts. After his debarment, Skiscim allegedly continued to bid, contract, and supply defective airplane parts to the federal government through a series of shell companies using the names of relatives and fictitious people to mask his involvement. During that time, his shell companies allegedly received more than $2.8 million for the supply of airplane parts, including parts shown to be defective. Not surprisingly, in prosecuting this case under criminal law, the US Government took very seriously the allegations that the defendant had not only violated the law but also risked the lives and safety of military personnel relying on those defective parts in military aircraft. *See United States v. Skiscim*, 16-cr-00190-ADS-AKT (E.D.N.Y. 2016).

- **Sentencing of Owner of Rhode Island Electronics Parts Company**

On January 21, 2016, the US District Court for the District of Connecticut sentenced Jeffrey Warga to three years of probation and ordered him to pay a $10,000 fine for supplying customers with falsely remarked microprocessor chips, many of which were used in U.S. Military and commercial helicopters. According to court documents and statements made in court, Jeffrey Krantz was the CEO and an owner of Harry Krantz, LLC, a New York-based company that allegedly bought and sold, among other things, obsolete electronic parts for use by the US military and commercial buyers. Krantz entered into a business relationship with Warga, the president and owner of Rhode Island-based Bay Components, LLC, to place those obsolete parts into the supply chain that ultimately led to the use of those chips in, inter alia, the assembly of US military and commercial helicopters. *See United States v. Warga*, 14-cr-00240-MPS (D. Conn. 2016).

VII. Cybersecurity

Government contractors are subject to an increasing – and fast moving – array of restrictions related to cybersecurity. Many of those restrictions focus on prime contractors' supply chains because each level of the government contracting chain is a potential point of cyber risk for the government customer. The regulatory environment regarding cybersecurity is in a state of very rapid evolution, and is at its most advanced in the Department of Defense (DoD). Accordingly, coverage in this Toolkit is a brief snapshot of several of the major requirements that exist as of December 2016 – contractors (and subcontractors) are encouraged to review the full text of applicable clauses. More changes are expected in coming months. And, of course, contractors that perform classified work have various additional requirements to which they (and their cleared subcontractors) are subject.

A. DFARS Supply Chain Risk Rule

Contractors' supply chains continue to be a focus of DoD regulatory interest. On October 30, 2015, DoD adopted as final, with certain key changes, an interim rule released in 2013 that implemented mandates found in the National Defense Authorization Acts (NDAA) for Fiscal Year (FY) 2011 and FY 2013 and amended the Defense Federal Acquisition Regulation Supplement (DFARS) to include DFARS Subpart 239.73 entitled "Requirements Relating to Supply Chain Risk." *See* 80 Fed. Reg. 67243 (Oct. 30, 2015).

This final rule should be given careful attention by defense contractors because it requires that DoD agencies use supply chain risk as an evaluation factor under certain procurements and allows DoD to exclude contractors due to such risk in procurements related to National Security Systems (NSS). In addition to addressing NDAA mandates, this DFARS subpart also addresses elements of DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)."

Contractors should note that this final rule is a further manifestation of the continuing strong focus on risk in the supply chain, and it is an example of the lead position that DoD has taken in addressing such risk.

B. Covered Defense Information/Network Penetration Reporting Rule

Over the past several years, DoD regulations have been evolving to implement sections of the FY 2013 and 2015 Defense Authorization Acts to require the safeguarding of, and "cyber incident" reporting by, certain defense contractors which have "covered defense information" residing in or transiting through "covered contractor information systems," including an initial rule issued in November 2013, two interim rules issued in August and December 2015, respectively, and a final rule issued in October 2016. These regulations are primarily implemented under DFARS Subpart 204.73 (Safeguarding Covered Defense Information and Cyber Incident Reporting) and two DFARS clauses, DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) and DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting).

On October 21, 2016, the DAR Council issued the final DFARS "Network Penetration Reporting" Rule. 81 Fed. Reg. 72,986 (Oct. 1, 2016). The rule, effective on the date of its issuance, involves changes in the key contract DFARS clauses, but also includes changes to several other DFARS provisions, for the stated purpose of improving contractors' notice of the rule's security and reporting requirements.

The final rule retains most of the key elements of the prior interim rules, including mandatory contractor and subcontractor reporting within 72-hours of cyber incidents involving systems containing "covered defense information" and contractor implementation of the National Institute of Standards and Technology (NIST) standards for protecting controlled unclassified information (CUI) on non-federal information systems under NIST SP 800-171 (or approved alternatives).

In earlier iterations of this rule, DoD had required the immediate implementation of certain NIST standards for safeguarding covered defense information, citing an urgent need to protect government information from cyber threats. In response to substantial complaints from industry, however, DoD adopted a phased-in approach to implement the NIST standards, calling for implementation of those standards "as soon as practical, but not later than December 31, 2017," while at the same time continuing to require rapid reports of breaches. The final rule continues to reflect this December 31, 2017 date for implementation.

The final rule does contain some notable changes and refinements. In particular, the October 2016 rule's coverage is broader than prior iterations because its definition of "covered defense information" encompasses all types of information called out in the National Archives and Records Administration's Controlled Unclassified Information (CUI) Registry discussed in Section D below, e.g., controlled technical information, export controlled information, and several dozen other categories and subcategories of sensitive but unclassified information. As discussed above, like the interim provisions in 2015, the final rule continues to require contractor implementation of NIST SP 800-171 (or approved alternatives) before the end of 2017. Under the FAR rule described in Section C below, however, contractors will likely need to implement 15 of the 100+ requirements more expeditiously and – until December 2017 – are immediately required to provide "adequate" security. Notably, the October 2016 final rule excludes COTS procurements from its coverage, but does not carve-out commercial item procurements.

The rule's implementation of DFARS clauses contains full text flow downs of those clauses under which subcontractors are obligated to (i) implement the safeguarding requirements for covered defense information (where subcontract performance will involve "covered defense information" or involve "operationally critical support"); (ii) notify the prime contractor (or next higher-tier subcontractor) if the subcontractor submits a request to vary from the NIST SP 800–171 security requirements to the Contracting Officer; and (iii) report any cyber incidents to DoD (while also informing the prime contractor of the existence of any such report). Some aspects of the rule may pose particular challenges for non-US subcontractors that may have concerns about directly reporting a cyber incident to US DoD.

C. FAR Contractor Information Systems Rule

On May 16, 2016, four years after issuing a proposed rule, the FAR Council issued a final cybersecurity-related rule that reaches deep into the supply chain and is applicable to virtually all government contractors and subcontractors. Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30,439. The rule establishes a new FAR subpart 4.19 and contract clause 52.204-21, both of which are entitled "Basic Safeguarding of Covered Contractor Information Systems." The rule is effective for solicitations issued on or after June 15, 2016.

The final rule imposes 15 safeguarding requirements that apply to contractor information systems, as opposed to focusing on specific types of information maintained by government contractors (which had been the focus of the proposed rule and is the focus of the DFARS rule described above). It is meant to be broad in scope and to supplement, rather than supersede, other cybersecurity requirements that may apply to government contractors, such as the DFARS rule. The new FAR clause is required to be included in contracts and subcontracts at all tiers, including contracts and subcontracts for commercial items (except COTS items), where the contractor or subcontractor may have Federal contract information in or transiting through its information system. The clause effectively sets baseline standards for protecting non-public information relating to US government contracts. Indeed, the rule's preamble states that its requirements are steps that "prudent" businesses would take irrespective of whether there was a FAR clause containing such requirements. The drafters recognize that the final rule is a building block in an evolving set of cyber-related rules (including more stringent rules regarding controlled unclassified information and classified information) and expect the requirements to be the "floor" rather than the ceiling for government contractors.

Although many contractors are already likely to be in compliance with the requirements of the rule (many of which are phrased sufficiently broadly to allow flexibility in implementation), some of the requirements may be new to smaller contractors and subcontractors only tangentially involved in government contracting. Moreover, the rule includes some ambiguities, such as the reference to "reporting" in Requirement 12. Perhaps more significantly, each of these requirements is drawn from NIST SP 800-171, which many defense contractors have been assessing for purposes of compliance with the DFARS Safeguarding clause discussed in Section B above and which gives contractors until December 2017 to complete implementation. Thus, as a result of the FAR rule, covered defense contractors no longer have until the end of 2017 to implement 15 of the 100+ NIST SP 800-171 requirements; instead they needed to have taken steps to implement the 15 requirements called for by the FAR rule by the middle of June 2016, just as did civilian agency contractors and subcontractors not subject to the DFARS rule. Finally, as with the DFARS provision, there is no explicit enforcement mechanism embedded in the clause

D. NARA Controlled Unclassified Information Rule

On September 14, 2016, the National Archives and Records Administration (NARA) issued a final rule regarding controlled unclassified information (CUI), effective November 14, 2016. Controlled Unclassified Information, 81 Fed. Reg. 63,324 (Sept. 14, 2016). The rule applies only to federal agencies, but states that it is important to protect CUI in non-federal information systems as well, and calls for agencies to implement their own procedures and

agreements to apply the rule's requirements to contractors and other non-federal entities such as grantees, universities, and state and local governments.

The NARA rule implements Executive Order 13556, Controlled Unclassified Information, and is part of the Government's effort to create a unified system for the treatment and identification of CUI that relates to government programs, i.e., to rein in and centrally organize the patchwork of categories and rules that have grown up over the years regarding sensitive but unclassified information. The rule cross-references NARA's formal "CUI Registry" and says that it will be the clearinghouse for categorization of such information. To the extent that a category of CUI information is subject to specific pre-existing legal or regulatory controls, that category will be known as "CUI Specific" and the pre-existing rules regarding its treatment will continue to apply. To the extent that categories of information exist which are not subject to pre-existing rules, those categories will be known as "CUI Basic" and baseline procedures specified in various NIST standards incorporated by reference in the rule will be applicable.

Several sections of the rule and preamble respond to both public and agency comments requesting further explanation on issues, or otherwise discuss how the different levels of CUI interact, the basis for CUI controls, the levels of control agencies may impose within the agency and outside the agency, the rules governing written agreements and information sharing, how to treat legacy information, destruction options, controls on dissemination, and reporting of mishandling.

Categories

The final rule identifies four categories of information provided by or developed for the Government:

Classified Information: Information required by Executive Order 13526, "Classified National Security Information," or predecessor or successor orders, or the Atomic Energy Act of 1954, to be marked with a classification designation to protect it from unauthorized disclosure.

CUI Basic: Information created or possessed by or for the Government where a law, regulation, or policy requires or permits safeguarding or dissemination controls. CUI Basic information is CUI for which no particular controls are specified – in effect, the default position. The rule gathers a majority of CUI under one set of consistent requirements, referred to as CUI Basic, and standardizes how agencies throughout the executive branch should comply. The rule also points out that this structure, the CUI Registry, NIST standards, and oversight functions by the CUI EA, are designed to restrain broad application of controls on information. The rule's uniform handling controls for CUI Basic require protection at no less than a "moderate" confidentiality standard under the Federal Information Systems Modernization Act (FISMA). CUI Basic documents can be marked simply as "CUI" or "Controlled."

CUI Specific: Information where applicable law, regulation, or policy provides specific handling controls that differ from the controls that would apply to CUI Basic. The final rule provides that those specified controls are to be followed for CUI Specific information and that applicable special markings should continue to be used on, for example, export controlled,

critical infrastructure, proprietary information or source selection information, to name just a few of the several dozen categories/subcategories of information listed on the registry which are subject to CUI Specific controls. The CUI registry will dictate the particular markings, and non-standard markings will not be allowed.

Uncontrolled Unclassified Information: Information that is neither classified nor CUI. Even though this information is not controlled or classified, it must still be handled as required by FISMA, which is the legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.

As indicated, as of November 14, 2016, the NARA rule applied directly only to federal agencies themselves. There is accompanying guidance and a timetable on the NARA website for the process by which agencies will develop the appropriate mechanisms for compliance and oversight, training, etc. Many of these requirements (including the implementation of agency-specific policies), take effect within 180 days of November 14, though some have a longer threshold. The CUI Registry currently notes that existing agency policies continue to apply until such time as each agency implements the NARA CUI rule. Among other challenges, there will be a significant burden on agencies to re-mark large quantities of pre-existing CUI, particularly when it is disseminated externally.

In due course, the rule will be indirectly applied to non-federal entities. To this end, the rule calls for agreements between non-federal entities and the Government to incorporate by reference the elements of the rule. With respect to civilian agency contractors, the rule is expected to be implemented through an upcoming FAR clause, which will presumably contain a flow-down provision. Moreover, as applied to defense contractors, some aspects of the final rule are effectively already implemented as a result of the DFARS Network Penetration Rule, discussed above, which calls for contractor implementation of NIST 800-171 standards and 72-hour reporting of breaches. It is possible that some agencies may implement specific requirements sooner.

E. Intelligence Community Directive

The Intelligence Community (IC) also is taking a leadership position in identifying supply chain cyber risks. The IC now operates under its Directive called "Supply Chain Risk Management" (ICD 731), which outlines the duties and responsibilities to protect the supply chain. This Directive defines the role of supply chain risk management within the IC and is intended to complement other supply chain risk management programs throughout the US Government.

F. China Sourcing Restrictions

The continuing resolutions to fund certain federal agencies for fiscal years 2013 through 2016 have included provisions that reflect the concern of Congress with risks posed by technology from the People's Republic of China. Those resolutions have prohibited Commerce, Justice, NASA and the National Science Foundation from purchasing certain types of IT systems "produced, manufactured or assembled" by entities "owned, directed, or subsidized by the

People's Republic of China" unless the head of the purchasing agency consults with the FBI and a determination is made that the purchase is "in the national interest of the United States."

VIII. Country of Origin and Related Restrictions

Several statutes and regulations impose country of origin restrictions on products sold to the United States Government. The most important are the Buy American Act (BAA) and the Trade Agreements Acts (TAA). These restrictions can have significant supply chain implications. Other significant laws and regulations, such as the Berry Amendment and US economic sanctions, also can have a significant supply chain impact.

A. Buy American Act (BAA)

The BAA, 41 U.S.C. §§ 8302-8305, applies to contracts for supplies for use within the United States that are above the "micro-purchase threshold" (currently $3,000). However, the BAA does not apply to acquisitions to which the TAA applies, and, in practice, most acquisitions of supplies should be subject to the TAA rather than the BAA.

The BAA restricts, but does not prohibit, the acquisition of supplies that are not "domestic end products." The BAA uses a two part test to determine whether a manufactured end product is "domestic:" (1) the end product must be "manufactured" in the United States and (2) the "cost of its components" produced or manufactured in United States must exceed 50% of the cost of all components. FAR 25.003 defines a "component" in relevant part as an "an article, material, or supply incorporated directly into an end product," and prescribes rules for determining the "cost" of components that are purchased and for those that are manufactured by the contractor. The FAR does not define "manufactured;" however, case law provides some guidance. The test for determining if an end product is "domestic" is relaxed for Commercial Off-The-Shelf (COTS) items; in those cases, the item must be "manufactured" in the United States but does not need to meet the 50% US cost of components test.

There are several exceptions to the BAA which permit the Government to acquire a "foreign end product." These include "nonavailability" and "unreasonable price" of a domestic end product. The BAA also does not apply to the acquisition of "information technology" that is a commercial item. Finally, the DFARS allows DOD more flexibility through the concepts of "qualifying country end product" and "qualifying country end component," as defined and explained in 252.225-7000 and 252.225-7001.

B. Trade Agreements Act (TAA)

The TAA, 19 U.S.C. § 2501, et seq., and FAR Subpart 25.4, generally restricts the Government's purchase of products (and services) to only "US-made" or "designated country" end products (and services). "Designated countries" are countries that are signatories to the World Trade Organization Government Procurement Agreement, countries with which the United States has free trade agreements (e.g., NAFTA) that provide for reciprocal non-discriminatory treatment for public procurement purposes, and certain developing and Caribbean Basin countries. Countries such as China and India are currently not "designated countries." The TAA applies to most acquisitions of supplies and services with an estimated value of more than $191,000 and to contracts for construction that exceed $7,358,000, although some trade agreements have different dollar thresholds and there are some procurements that are exempt from the TAA.

FAR 25.401 provides that the TAA does not apply to certain acquisitions, for example, those set aside for small businesses; most acquisitions that are exempt from full and open competition under FAR parts 6.2 or 6.3; and certain national defense related procurements. The TAA also provides for "nonavailability" determinations. However, the TAA ***does apply*** to contracts for commercial items, including GSA Multiple Award Schedule contracts, and, unlike the BAA, does not include an exception for commercial information technology. Finally, the TAA clause at DFARS 252.225-7021 permits acquisitions from "qualifying" as well as from "designated" countries.

Under the TAA, a "US-made" end product is one that is either (1) "mined, produced or manufactured in the United States," or (2) "substantially transformed in the United States into a new and different article of commerce with a name, character or use distinct from that of the article or articles from which it was transformed." DFARS 252.255-7021. "Designated country end product" is similarly defined – the end product is wholly the growth, product or manufacture of a designated country, or was "substantially transformed" in a designated country. DFARS 252.255-7021.

"Substantial transformation" for TAA purposes is determined on a case-by-case basis considering the "totality of the circumstances," including:

> The country of origin of the item's components, extent of the processing that occurs within a country, and whether such processing renders a product with a new name, character, and use are primary considerations in such cases. Additionally, factors such as the resources expended on product design and development, the extent and nature of post-assembly inspection and testing procedures, and worker skill required during the actual manufacturing process will be considered when determining whether a substantial transformation has occurred. No one factor is determinative.

CBP HQ Ruling H215555, July 13, 2012; *see also* FAR 25.001(c)(2).

For many products which include material or components from different countries, final assembly will often be found to transform the inputs into a new and different product with a different name, character or use, and thus determines the country of origin. Additional considerations can apply in determining the country of origin of computer equipment and intangible software. Moreover, as noted above, no one factor is necessarily determinative of country of origin and other factors such as the complexity of the assembly process, the place where the engineering, research and development were performed, and the origin and value of key components can affect the outcome. In addition, the relative value and complexity of the inputs also can be relevant in determining the final product's country of origin.

C. Supply Chain and Compliance Considerations

Country of origin requirements, such as the BAA and TAA, can have significant supply chain implications. For example, procurements subject to the BAA require careful analysis of the bill of material of the end product to ensure that the components meet the US content requirements. Where the TAA applies and the end product is not wholly the product of the

United States or a single designated country but is sourced from more than one country, the contractor should determine where substantial transformation occurred in light of applicable rulings from the Bureau of Customs and Border Patrol, or seek a country of origin determination from Bureau of Customs. A reseller should consider obtaining a representation or certification from its supplier as to the end product's country of origin. Case law indicates that a contractor can rely on a supplier's representation regarding country of origin, provided that the reliance is reasonable. *See United States ex rel. Folliard v. Government Acquisitions, Inc. & Govplace*, 764 F.3d 19 (D.C. Cir. 2014). As a result, prime contractors should be alert for red flags or potential issues and consider taking other steps to demonstrate reasonable reliance. Likewise, suppliers should be attentive to the accuracy of such representations to avoid potential liability to the contractor and potentially the Government. Some prime contractors also require suppliers to agree to indemnify them for liability due to allegedly false certifications.

Country of origin provisions in the BAA and TAA are implemented through solicitation provisions and contract clauses. For example, where the TAA applies, FAR 52.225-6 requires the offeror to certify that the end products to be delivered are either US-made or designated country end products, and to identify those, if any, which are not. FAR 52.225-2 includes a similar certification regarding BAA compliance. Country of origin requirements in the TAA and BAA therefore should be addressed prior to proposal submission and contract award and should be approached with care.

BAA and TAA non-compliance can present significant issues for contractors. For example, bid protests challenging compliance with the TAA are becoming more frequent, and a number of those protests have been successful. Downstream, the courts and boards have upheld terminations for default based on BAA and TAA non-compliance. Non-compliance with the country of origin requirements in the BAA or TAA, including improper certifications of compliance, also can result in government or *qui tam* actions under the civil False Claims Act (FCA) and there have been a number of multi-million dollar settlements of FCA cases arising out of alleged violations of the TAA. Criminal or civil fraud proceedings also can give rise to administrative actions for suspension or debarment from government contracting.

D. Other Restrictions

Although they are probably the most frequent, the BAA and TAA are not the only country of origin rules applicable to government procurements. For example, the Berry Amendment essentially requires DOD to buy certain textile and specialty metal products that are 100% domestic in origin, but there are certain complicated exceptions to this basic requirement. The Berry Amendment is implemented in DFARS Subpart 225.7002. The American Investment and Recovery Act also includes its own Buy American provision. There are also Buy American type restrictions applicable to federal assistance programs (grants) for transportation projects such as highways, transit systems and airports. In addition, contractors that work with the US Agency for International Development (USAID) should be aware that USAID has special rules found at 22 C.F.R. § 228 entitled "Source and Nationality" (formerly "Source, Origin and Nationality") that also can impact sourcing decisions and may restrict where items or services are purchased, though these rules no longer relate directly to country of origin.

E. 2016 Update

1. Regulatory Developments

Like the GSA, the Department of Veterans Affairs (VA) has a multiple award schedule contracts program, including contractors offering medical equipment, supplies and pharmaceuticals, and the VA has required those products to be TAA compliant. In April 2016, the VA made an exception and issued a "non-availability" determination under which it required certain "covered drugs" to be available (under its Schedule 65 I B) without regard to TAA compliance. Unavailability determinations usually turn on a finding that TAA compliant products are not available in sufficient quantities to fulfill the Government's requirements. In this case, however, the VA relied on a statutory direction that the "covered drugs" at issue must be available for sale under the Schedule 65 I B schedule contracts and required manufacturers of those drugs to make them available under their contracts.

2. Case Law

In a case of first impression, the United States Court of International Trade recently addressed "substantial transformation" for purposes of determining country of origin for US government procurement purposes under the TAA. *Energizer Battery, Inc. v. United States*, 2016 WL 7118538 (Ct. Intl. Trade 2016). The Court noted the dearth of judicial opinions addressing this issue under the TAA and looked to cases arising under other statutes with identical language. It recognized that the test for whether there has been substantial transformation is fact specific and looks to whether "'a new and different article [has] emerge[d], having a distinctive name, character, or use.'" With respect to change in character, it noted that "when the post-importation processing consists of assembly, courts have been reluctant to find a change in character, particularly when the imported articles do not undergo a physical change." With respect to change in use, it stated that courts have "found that such a change occurred when the end-use of the imported product was no longer interchangeable with the end-use of the product after post –importation processing," but that "when the end-use was predetermined at the time of importation, courts have generally not found a change in use." Finally, it also pointed out that courts have considered various "subsidiary or additional factors, such as the extent and nature of operations performed, value added during post-importation processing, a change from producer to consumer goods, or a shift in tariff provisions," but that there is no uniform or exhaustive list of those factors and that consideration of them "is not consistent."

3. Compliance: Customs Rulings and Software Development

As previously noted, compliance with US country of origin requirements and domestic preferences can present compliance challenges for contractors in a world of global supply chains. One way to obtain assurance on TAA compliance is to obtain either an advisory ruling or final determination on country of origin from the US Customs and Border Patrol (Customs). Over the past year, Customs has issued rulings on a wide range of products, including computer software, intermodal containers, multi-function printers, exercise equipment, pharmaceutical products, and even billiard tables.

For example, computer software products are often developed in multiple countries, including some, such as India, that are not TAA countries. In determining country of origin of software, Customs considers the overall software development process and where (in which countries) the different steps in that process take place. Most importantly, it has singled out the "software build" – the compilation of source code into object code – as the step that results in "substantial transformation" and has thus found that the country of origin for government procurement purposes is where the software build occurs. See Customs Advisory Ruling, Country of Origin of Imported Software, No. HQ H192146 (June 8, 2012). We also issued a Steptoe advisory addressing this and other such rulings by Customs, which can be found here: Steptoe & Johnson, LLP, *Country of Origin Requirements for US Government Procurements: Intangible Software* (May 8, 2014).

4. Enforcement

Country of origin non-compliance also continues to be the subject of Government scrutiny and enforcement, including actions by contracting agencies, criminal proceedings, and actions under the civil False Claims Act (FCA).

a. GSA Administrative Action

In 2016, GSA emphasized compliance with the TAA on its Multiple Award Schedule (MSA) contracts and "requested" that all GSA MAS contractors review their contract pricelists to confirm compliance with the TAA and the accuracy of their certification of TAA compliance. The notice from GSA did not require contractors to provide additional information regarding TAA compliance but did direct them to delete any non-compliant products from their contracts. GSA also suggested that resellers "may need to confer with the manufacturer, OEM, or wholesaler." GSA's notice reminded contractors that they were responsible for ensuring the accuracy of product information and concluded by stating that "implementing a system to ensure compliance is both a best and a wise practice."

GSA's request was apparently prompted by Congressional inquiries about the alleged inclusion of non-TAA compliant products on GSA MAS contracts and followed an earlier GSA letter to a large number of GSA schedule contractors regarding compliance with TAA (and "Made in America") requirements for products listed on GSA Advantage. GSA's earlier letter directed those contractors to verify TAA compliance for every product on their MAS schedules by providing a copy of either a Certificate of Origin or certification of compliance from the manufacturer.

In taking these actions, GSA has emphasized the importance of TAA compliance. As GSA's initiatives suggest, GSA MAS contractors should consider implementing processes for ensuring that such certifications are accurate and that the products on their MAS contracts are TAA compliant, particularly because non-compliance could result in serious consequences for the contractor, including cancellation as well as potential claims under the FCA.

b. Bid Protests

In *Bunzl Distribution California, LLC*, B-412475.4, 2016 CPD ¶ 314 (Oct. 21, 2016), the GAO upheld a Contracting Officer's determination that Bunzl was not responsible under FAR

Subpart 9.1. That determination was based on Bunzl's failure to demonstrate its TAA compliance, including the failure to provide letters of supply for certain items, failure to identify country of origin on other letters of supply, and failure "'to demonstrate[] that it had or would have the capability to comply with TAA sourcing requirements'" for about 10% of the items to be supplied under the contract. Responsibility determinations receive substantial deference at GAO and, as a result, it is difficult to overturn a negative responsibility determination. The CO's review of the offeror TAA compliance was triggered by a previous protest by another offeror, and ultimate awardee, alleging, among other things, Bunzl did not comply with the TAA.

c. Criminal and FCA Cases

In June 2016, a Wisconsin based producer of architectural structures used in public projects pled guilty and paid a $500,000 fine to resolve allegations that it had repackaged material and falsified documents to hide that it was using non-compliant foreign material, including material from China, on federally-funded construction projects on which it was a subcontractor. According to the plea agreement, the company also agreed not to contest proceedings to debar it from government contracting. In addition, it agreed to pay another $2.5 million to settle a parallel FCA qui tam case that alleged violations of the Buy American Act and American Resource and Recovery Act.

In another case, a UK-based manufacturer of custom racking systems pled guilty to intentionally concealing and failing to mark products imported from China to make it appear that the products were BAA and TAA compliant. It also paid a forfeiture of just over $1 million as part of its guilty plea.

GSA MAS contract holders also continue to be at risk of FCA actions. Earlier this year, a court in Illinois unsealed a qui tam complaint filed by a competitor against several other GSA schedule contractors after the DOJ declined to intervene and prosecute the case. The complaint alleged that the contractors had falsely certified that products sold under their Schedule contracts were TAA compliant.

F. Other Restrictions

Federal assistance programs (grants) for transportation projects are also subject to Buy American type requirements. In December 2015, the US District Court for the District of Columbia set aside a 2012 Federal Highway Administration (FHWA) Policy Memorandum which had provided that iron and steel manufactured products containing less than 90% iron and steel and all "miscellaneous steel or iron products" were exempt from the applicable Buy America requirement. As the Court observed, under the FHWA Policy, a manufactured product that contained no more than 89.9% steel or iron could have been obtained from a foreign source, and a faucet, bolt or similar miscellaneous items could consist of 100% foreign steel or iron. The Court held that these exemptions should have been subject to rulemaking requirements, including public notice and comment, and that the FHWA had otherwise failed to justify its 90% rule for manufactured products. The lawsuit challenging the FAA policy was brought by a group of interest parties, including a union, domestic steel and iron product manufacturers, and an industry association. The FAA subsequently cancelled its 2012 Policy Memorandum.

IX. Export Controls

US Government contractors are increasingly engaged in opportunities abroad, whether for the US or foreign governments, as well as relying on a growing global supply chain for domestic US Government programs. Increased overseas contracting, however, brings with it compliance risk, particularly as contractors deal with non-US subcontractors and suppliers. Much of the compliance risk is associated with US export control laws that are predominantly outside the Federal Acquisition Regulation (FAR) system with which US Government contractors are comfortable. Contractors also should note that economic sanctions are a related area of supply chain risk and briefly covered in this Toolkit's Country of Origin section.

The United States has two primary sets of export control laws and regulations—the International Traffic in Arms Regulations (ITAR), administered by the State Department, and the Export Administration Regulations (EAR), administered by the Commerce Department. (The Department of Energy and the Nuclear Regulatory Commission also have export controls.) In general, the ITAR are defense-related export controls. The EAR are primarily dual-use-related controls but now, as a result of recent reform efforts, control some military items. A wide variety of activities can constitute exports, such as: shipping items from the United States; personally carrying controlled technical data out of the United States on an electronic device such as a tablet; transmitting information electronically by any means; allowing access by foreign persons (a term defined in the ITAR and EAR) to company networks, directories, etc. with controlled technology; and releasing controlled data during spoken conversations. An export also can include disclosure of the US-controlled technical data to foreign persons in a variety of procurement-related activities, such as sharing technical data with actual or potential US suppliers which employ foreign persons, transmitting such data to foreign entities, including affiliates or subsidiaries, or transmitting such data through entities that support offset requirements imposed by foreign governments. The ITAR and EAR also control "reexports or retransfers," in which an item subject to US jurisdiction is shipped or transmitted from one foreign country to another foreign country, or to an unauthorized user in the same foreign country.

A. The ITAR

The State Department's Directorate of Defense Trade Controls (DDTC) regulates the export and temporary import of "defense articles" and "defense services" through the ITAR. The US Munitions List (USML), published in the ITAR, sets forth 21 categories of controlled defense articles and defense services.

Defense articles include hardware, technical data, and software that are specifically (or now, as a result of export reform, "specially") designed, developed, configured, adapted, or modified for a military, space, or intelligence application not controlled by or subject to the EAR (i.e., do not have a predominant civil application/performance equivalent). The ITAR do not simply regulate end items, but they also regulate USML-controlled parts and components incorporated into or attached to any item (including defense articles), wherever developed or manufactured. Controlled technical data is information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of

defense articles. It may include drawings, design specifications, software, photographs, and work instructions.

Defense services include the furnishing of assistance by a US person to a foreign person, wherever located, with respect to ITAR-controlled defense articles, and the furnishing of any ITAR-controlled technical data associated with a defense article. Defense services may be provided through, among other things, training, technical support, and testing.

The ITAR obligate contractors to obtain export licenses or approvals for exports, reexports, or retransfers of controlled defense articles, technical data, and services from the United States to every country in the world or to a foreign person. Special license exemptions exist for certain Canadian transactions and recent treaties involving the United Kingdom and Australia may result in similar treatment for certain programs and export/reexport-related activities involving those countries. Formal export licenses are generally required for exports of hardware. Exports of technical data and services are typically authorized pursuant to, and exemptions in furtherance of, "technical assistance agreements" (TAAs) or "manufacturing license agreements" (MLAs). See DDTC Agreement Guidelines. Companies involved with ITAR defense articles and services are usually obligated to become registered with DDTC, even in circumstances in which they merely manufacture such ITAR-controlled defense articles in the United States (rather than export those articles). *See* DDTC Registration Guide. Registration also is required for brokering activities related to defense articles and defense services, such as facilitating foreign sales. Registration obligations include provision of information regarding ownership (including foreign ownership, control, and influence) as well as the designation of an "empowered official" to manage licensing and compliance issues for the company. Registration does not independently provide for any export authorization. Finally, in certain circumstances, license applicants, vendors, and suppliers must report information about fees, commissions, and political contributions paid, or offered to be paid, to persons or government officials for the provision of defense articles or defense services to the armed forces of a foreign country.

The ITAR (and companion EAR provisions) are in the process of being revised because of a US Government export reform initiative, which began to be implemented in 2013 and will continue for the next few years. Therefore, certain items previously covered by the ITAR and still considered to be defense articles are being transitioned from the USML to the Commerce Control List of the EAR because they no longer warrant as strong controls, but still may require licenses for exports and reexports to destinations that are not close US allies.

B. ITAR: Supply Chain Compliance Considerations

Contractors need to be aware of the ITAR at all stages of an opportunity, whether for a US agency customer, a foreign government (either as a direct commercial sale or as part of the Foreign Military Sales program), or a US or foreign prime contractor. ITAR compliance is particularly complex to manage with a multi-layered supply chain when it may be necessary to share know-how or technical information across borders (or with foreign persons in the United States).

From a compliance perspective, it is important to recognize that neither the ITAR nor the EAR are incorporated directly in the FAR system, except for a DFARS provision at 225.7901-3

that specifies the need to comply with export controls (and refers to the EAR and ITAR by name) and implicitly raises a possibility that a violation of export controls might be considered a contract violation. This clause is a mandatory flow down. In a US Government supply chain setting, however, prime contractors also should consider creating their own "bespoke" export control clauses that supplement the DFARS provision. This is important with domestic subcontractors and suppliers as well as foreign entities. Foreign suppliers and subcontractors also may need to enter into "Technical Assistance Agreements," which are separate and apart from their main subcontracts, in order to receive export controlled technical data and collaborate with US entities higher up the supply chain.

Violations of the ITAR are normally handled administratively by DDTC, though recently DOJ's National Security Division published guidelines encouraging the self-reporting of potential criminal violations of export control rules to DOJ. *See* DOJ's Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation In Export Control And Sanctions Investigations Involving Business Organizations (Oct. 2, 2016). Because of export reform, companies may need to consider both the ITAR and EAR implications of a potential improper export. In addition, contractors should be mindful of the possible interplay between export control voluntary disclosure regimes and the DFARS rule requiring the reporting to DoD of cyber incidents involving export controlled information, including the reporting of such cyber incidents by subcontractors downstream in the supply chain (by virtue of a flow-down clause). *See* DFARS Subpart 204.73; DFARS 252.204-7012.

C. Export Administration Regulations (EAR)

The Bureau of Industry and Security (BIS) of the Commerce Department administers the EAR, which controls the export of dual-use technologies through the Commerce Control List (CCL). Dual-use items are commodities, software, or technology that have both a commercial and military application, and are assigned an Export Control Classification Number (ECCN) on the CCL. Defense articles (including commodities, equipment, materials, software, and technology) no longer on the USML, but warranting export restrictions, are enumerated in the "600 series" of the CCL (items related to satellites are anticipated to be found in the 500 series). Unlike the ITAR, which control exports to essentially all counties, an item subject to the EAR can be controlled (i.e., require a license) for some countries, end users, and end uses but not others. In many instances, items can be exported to closely allied countries license-free or using an applicable license exception. Special (and complex) rules apply to exports of encryption software and related technology.

Export activities controlled by BIS (and DDTC) include not only the permanent or temporary shipment or transmission of an item outside the United States, but also the transfer of hardware or controlled technology to foreign persons within the United States (known as "deemed exports") or to dual/third country nationals of foreign host countries outside the United States (known as "deemed reexports"). In certain circumstances, the EAR may restrict the application abroad of technical assistance (e.g., training) by a US person involving certain controlled technology or specific end uses (e.g., chemical and biological weapons).

D. EAR: Supply Chain Compliance Considerations

Almost everything that is not subject to the ITAR is likely subject to the EAR. The EAR, however, do not control all items for all locations. In many instances items that are controlled for certain reasons and destinations can be exported license-free, or subject to an exception, under the EAR. Nonetheless, depending primarily on the item and the country of the end user (or the member of the supply chain with which the US entity is contracting), licenses will sometimes be required.

Like the ITAR, there are several exceptions that impact government contractors when they are performing work either for the United States or an allied government. These are primarily exceptions for civil end users (i.e., nonmilitary known as "CIV"), servicing and replacement of parts and equipment (RPL), government and international organization end users (GOV), and the Strategic Trade Authorization (STA) (which is the result of recent export reform efforts). See 15 C.F.R. § 740.

X. Antiboycott Laws

A. Overview

Due to increasing concerns in the 1970s about efforts to pressure US companies to participate in or to support the League of Arab States economic boycott of Israel, the US Congress enacted antiboycott legislation to counteract the reach of the Arab League's boycott. The US Department of Commerce, Office of Antiboycott Compliance (OAC), and the US Department of the Treasury, Internal Revenue Service (IRS), administer separate antiboycott regulations. Although the regulations were first published in response to the Arab League boycott, the regulations are drafted broadly to discourage participation by US entities in ***any*** foreign boycotts or restrictive trade practices that the United States does not support. The antiboycott regulations make it illegal, or penalizable in some cases, for a "U.S. person" to support another country's boycott of a third country, which the United States does ***not*** sanction.

The OAC's antiboycott regulations apply to all "U.S. persons," including individuals and companies located in the United States and any foreign affiliate "controlled in fact" by a US company conducting business in the "interstate or foreign commerce of the United States." The IRS's antiboycott regulations apply to US taxpayers and their "controlled group."

In seeking the award of a contract from the US Department of Defense, a foreign offeror also may need to commit to the requirements identified in Defense Federal Acquisition Supplement (DFARS) 252.225-7031. This clause asks foreign offerors to certify that it "[d]oes not comply with the Secondary Arab Boycott of Israel" and that it "[i]s not taking or knowingly agreeing to take any action, with respect to the Secondary Boycott of Israel by Arab countries," which a United States person is prohibited from taking under US law. *Id.*

According to the most recent Treasury Department report, countries that may require participation in, or cooperation with, unsanctioned boycotts include Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, United Arab Emirates, and Yemen**.** The OAC does not publish a similar list of unsanctioned boycotts, but reports issued by the US Congressional Research Service over the past several years have identified boycott-related requests arising from a number of countries in the Africa, Middle East, and Southeast Asia regions, such as Bahrain, Jordan, Malaysia, Oman, Pakistan, among others. As a result, although many government contractors should include antiboycott compliance as part of their supply chain risk management program, this is especially important for those contractors that operate in or near these regions or that have supply chains with links to these regions.

B. Boycott Requests

"U.S. persons" are directed to report certain "requests" to participate in a boycott to OAC and/or the IRS. Failure to report receipt of such requests could be a violation of US law. Although certain exemptions may apply, and the specific facts of the transaction may determine whether there is an antiboycott problem or a reporting requirement, companies should be mindful of the following types of "requests" to support a third country's boycott:

- Not to do business with: (a) a boycotted country, (b) companies, nationals, or residents of a boycotted country, (c) other entities doing business with a boycotted

country, (d) so-called “blacklisted"” firms or persons, or (e) any other entity if you reasonably suspect the request is related to the boycott of such a country;;

- To do business only with approved firms or persons (for example, those on a so-called “white list”);
- To discriminate against US persons on the basis of race, religion, sex, or national origin;
- To inquire about a US person’s ancestry, national origin, religious identification, or parentage using the words “Israel,” “Hebrew,” “Jewish,” “Star of David,” or other words indicative of such background;
- To furnish data regarding a US person’s race, religion, sex, or national origin;
- To furnish information about anyone’s: (a) past, present, or future business relationships with a boycotted country, with companies, nationals, or residents of such a country, or with blacklisted persons, e.g., certifications that goods do not originate from Israel or blacklisted firms, or (b) association with charitable or fraternal organizations supporting a boycotted country; or
- To require or insist upon “compliance” with laws or regulations of a boycotting country, even if generally stated and whether or not there is a reference to “boycott” laws or regulations.

Boycott requests can be oral or written. These types of requests and restrictions can appear in any number of commercial-related documents, including but limited to requests for proposals, purchase orders, contracts, business registrations, freight and customs documents (Bills of Lading, Air Waybills, Certificates of Origin), financial documents, employee work related forms (such as visas, immigration, and work permits), or copyright and other licensing agreements. Specific examples of recent boycott requests are available on OAC’s website.

Although some of the requests described above may not be penalizable or constitute a violation, the examples, which are not exhaustive, reflect warning signals which should receive scrutiny for antiboycott compliance and could trigger reporting requirements. Therefore, to manage supply chain risks under US antiboycott laws, companies could potentially consider, among other steps, training personnel to be alert for any statements or requests (written or oral) that could indicate the presence of such boycott issues, to review commercial documents and communications to identify potential boycott “red flags,” and to present those requests to appropriate personnel for further evaluation and action, to include reporting.

Criminal and civil penalties and administrative sanctions for antiboycott violations (including the failure to report a request) may be imposed by OAC. OAC investigates and enforces civil violations of the antiboycott provisions. The US Department of Justice also may prosecute companies and individuals for intentional violations of these laws, including criminal penalties and potential imprisonment. The IRS regime also could result in penalizing companies

for cooperating in an unsanctioned international boycott, such as the loss of foreign tax credits, as well as penalties for failing to report such requests.

XI. Foreign Corrupt Practices Act (FCPA)/Anti-Corruption

US Government contractors performing work abroad face substantial risks under the US Foreign Corrupt Practices Act (FCPA), 15 U.S.C §§ 78dd-1 et seq., and the anti-corruption laws of relevant foreign jurisdictions. This may seem counterintuitive because the FCPA deals with bribes to "foreign" officials whereas US Government contractors work with US Government officials. However, even when performing a US Government contract, there are many opportunities for FCPA violations, particularly down the supply chain.

The FCPA criminalizes the bribery of "foreign officials" in order to obtain or retain business or secure any business advantage. The term "foreign officials" includes foreign government officials, employees of government instrumentalities (e.g., stated-owned or state-controlled enterprises), foreign political party officials, officials of public international organizations, and candidates for foreign political office.

The FCPA prohibits not only direct bribes to such persons, but also the making, authorizing, offering, or promising of payments to "any person"—in particular third parties such as agents, representatives, subcontractors and suppliers—with knowledge or reason to believe that the payments will be passed through, in whole or in part, to persons covered by the statute. In addition, the FCPA obligates US or foreign companies with publicly-traded securities in the United States to adhere to formal standards of recordkeeping, maintain internal controls reasonably designed to prevent bribery, and take other steps to ensure that the investing public is able to obtain a true and complete financial picture of their activities.

Within this framework, the FCPA presents some unique risks to companies and individuals subject to it. Most importantly (and by definition), the FCPA addresses conduct outside the United States. Its provisions can be applicable to virtually any company or person anywhere in the world, including in emerging markets (including key US allies) where public corruption may be common. The FCPA covers three classes of natural and legal persons: (1) US companies, citizens, and permanent residents (who face perhaps the most expansive prohibitions as they can be liable for FCPA violations across the globe simply by virtue of their nationality); (2) "issuers" of publicly-traded securities in the United States (whether equity or debt), as long as some act in connection with the prohibited payment touches the United States in some way or they fail to comply with the accounting and internal controls requirements; and (3) in certain circumstances any person, including non-US nationals and non-US corporations, where some act in furtherance of the prohibited payment occurs in the United States.

Government contractors operating abroad may need to retain or engage a variety of agents, consultants, subcontractors, joint venture partners, customs brokers, and others to navigate local business environments which may lack transparency. Accordingly, a significant source of risk under the FCPA for US government contractors is the use and control (or lack thereof) of third parties in the course of a company's business dealings. In other words, although contractors may not be the one making a particular payment, or the payment made by the contractor may not be made to a "foreign official" but rather a third party, the enforcement agencies might attempt to rely on theories of vicarious liability, including as applied to the FCPA's knowledge standard, to impute liability.

The third-party risks occur more frequently when contracting with a foreign government, either through direct contract sales or foreign military sales, than when contracting with the US Government for performance abroad. That is because agents/representatives and local partners may be required as part of the direct contracting regime of certain foreign countries or through the foreign military sales program.

However, the past few years have seen the rise of service contracts being performed abroad, particularly in support of contingency operations. These are particularly high risk for government contractors in light of the numerous corruption risks that contractors face in performing a contract. Among the many operations in which risks arise are the use of customs brokers, retention of security contractors, etc. This is true not only for US prime contractors but also for subcontractors. Service contracts also provide many opportunities for third parties to interact with foreign governments, even in support of a US Government contract, e.g., customs, tax and immigration officials of the host government.

As discussed above, US Government contractors face risks in connection with the prospect of legal liability for their own actions or the actions of entities in their supply chain. They also face potential collateral consequences for such violations in the form of debarment or other loss of business from the US, EU, and/or other governments. These risks can be managed, however, by adopting compliance solutions such as:

- **Design and implement FCPA compliance policies, procedures, and guidelines:** There is an increasingly well-developed body of standards that are acknowledged to meet companies' legal obligations under the FCPA to maintain effective internal controls to prevent bribery. Such policies and procedures should include baseline prohibitions on improper payments; procedures for making lawful payments to foreign officials; travel, entertainment, and hosting guidelines; a facilitating payments policy; policies for engaging security services, governments, and other risky third parties (including developing specific contract language providing for audit and other rights); "know your customer" policies; and others policies, procedures, and guidelines as appropriate. Policies should involve due diligence on the ultimate beneficiaries of payments, and the avoidance of dealings with politically exposed or other persons with a history of corruption, human rights abuses, or other behavior raising "red flags." Third party vetting, monitoring and auditing are particularly important from a supply chain perspective. The US Department of Justice (DOJ) and the Securities Exchange Commission (SEC) published a guide on these topics in 2012 that contractor's should consider reviewing. *See A Resource Guide to the US Foreign Corrupt Practices Act* (2012).

- **Develop strong financial controls:** Finance personnel should be trained to identify problematic payments or unclear records, ensure all payments comport with applicable laws, and know when to raise issues arising under the company's policies and procedures. Due to the FCPA's accounting requirements, this is particularly important for issuers.

- **Effective policy implementation:** The US enforcement authorities continue to place additional emphasis on communication and training on the requirements of a

company's FCPA compliance policies. Recent enforcement cases demonstrate that companies that train key employees—including all who interact with foreign government personnel, security services, and labor unions, and who make financial decisions—to recognize common FCPA risks will stand a much higher likelihood of avoiding potential compliance issues. Third parties such as agents, representatives, subcontractors and suppliers are increasingly being required by companies to attend training programs. Ensuring that there are knowledgeable company personnel available in real-time to provide guidance when questions arise is also an important component of an effective FCPA compliance program.

- **Reporting, investigation and remediation, and testing:** Significantly, companies are increasingly obligated to create mechanisms for employees and those in their supply chain to report problems. Companies that successfully encourage such reporting when FCPA concerns arise, and investigate and address those concerns, stand a lower likelihood of encountering problems in the future. Importantly, companies also should develop capacity internally and externally (through internal audit and outside counsel) to periodically test their FCPA compliance measures. Encouraging (or mandating) that suppliers have similar mechanisms is also prudent.

Of course, companies should adapt these compliance measures to their own operations and their own supply chains. Although these measures cannot prevent every potential violation or address every risk, they can equip companies with the tools to manage FCPA risks in challenging markets around the world. This in turn will protect the value of their overseas revenue flow, the company, and the employees themselves as they shift a higher percentage of their attention to non-US markets.

Finally, the FCPA is not the only anticorruption statute contractors will need to comply with when operating outside the United States. As part of their obligations under the OECD Convention Combatting Bribery, a number of other countries have implemented, updated, and/or began to more rigorously enforce transnational anticorruption laws in the last few years. Therefore, when a US contractor works abroad, it must be mindful not only of US laws that might implicate its conduct, but also of local laws and possibly third country laws. In 2010, the United Kingdom passed the Bribery Act 2010, c. 23 (Eng.), which is the United Kingdom's qualifying statute under the OECD convention. Although there has been relatively little enforcement of the Act to date, on its face, it arguably has a more expansive jurisdictional reach than the FCPA. It addresses a wider range of subject matter than the FCPA, including prohibitions against commercial bribery. Unlike the FCPA, the UK Bribery Act also contains a compliance-related affirmative defense, under which companies may argue that they maintained "adequate procedures" to prevent bribery, thus potentially protecting them against liability in the event improper payments are made by persons associated with the company.

The existence of the UK Bribery Act's "adequate procedures" defense highlights the importance of contractors implementing effective compliance policies when they operate abroad. Those policies are important not only to protect companies from FCPA liability in the United States, Bribery Act liability in the United Kingdom, or under countries' local laws, but also against other major trading nations' transnational bribery laws, such as Canada and Germany in particular, which have stepped up their own enforcement efforts in recent years.

XII. Combating Trafficking in Persons

US Government contractors (and subcontractors) must comply with Federal legislation and regulations issued to combat trafficking in persons. These "Combating Trafficking in Persons" (CTIP) rules are issued under Federal Acquisition Regulation (FAR) Subpart 22.17 and FAR 52.222-50. The CTIP rules supplement criminal prohibitions and penalties established under the Trafficking Victims' Protection Act.

The broad compliance regime in the CTIP rules addresses trafficking in persons in three areas that are important to managing government contractor and subcontractor supply chains:

1. It prohibits a range of activities related to trafficking in persons that are applicable to all government contracts and subcontracts, including commercially available off-the-shelf (COTS) items.

2. It creates an expanded reporting and enforcement mechanism for expanded prohibitions applicable to all contractors.

3. It imposes a broad set of compliance plan, due diligence and certification requirements for overseas contracts and subcontracts valued over $500,000.

A. Prohibitions Applicable to All Contracts

For more than a decade, the CTIP FAR clause at FAR 52.222-50 has included basic prohibitions against engaging in trafficking in persons. The prohibited activities include (a) engaging in severe forms of trafficking in persons, including using force or the threat of force in hiring, during the period of performance of a contract; (b) procuring commercial sex acts during contract performance; and (c) using forced labor in the performance of a government contract. In 2015, the CTIP FAR clause was expanded to prohibit contractors and subcontractors, and their employees and agents, from engaging in a range of other practices related to trafficking in persons in recruiting, hiring and employing, for both domestic and overseas contract performance. The prohibited practices include simple prohibitions on destroying, concealing, confiscating or otherwise denying access to the employee's identity or immigration documents; and more complex prohibitions, such as those relating to denial of payment for return transportation, which require a careful analysis of related rules for protecting employee victims and witnesses in trafficking investigations.

B. Awareness and Disclosure Commitments Contained in All Contracts

In addition to these prohibited activities, the CTIP FAR clause directs all government contractors to create an awareness program to inform employees about the prohibitions and potential punishments for violation of the policy. The CTIP FAR clause commits contractors to notify the Government when they receive "credible information" that a contractor employee, subcontractor, subcontractor employee or their agent has violated the CTIP regulations. The CTIP FAR clause also commits the contractor to provide "full cooperation" with government CTIP investigations and audits, which includes commitments to: (1) disclose credible information of any alleged violations of the CTIP regulations, sufficient to identify the nature

and extent of an offense and identify the potential responsible individuals, (2) provide timely and complete responses to auditor's and investigator's requests for documents, (3) provide reasonable access to facilities and staff to facilitate federal audits and investigations, (4) protect employees suspected of being victims of trafficking or witnesses, and (5) refrain from hindering or preventing employees from cooperating with US Government authorities.

The CTIP FAR clause is a mandatory flow down clause for all covered contracts. Thus, subcontractors must be knowledgeable about these prohibitions and commitments and monitor their own supply chains for compliance. Of course, contractors that try to monitor and enforce these requirements may encounter resistance from certain suppliers, which are not subject to the prime contractor's control, such as suppliers which might be competitors to a prime contractor and unwilling to share sensitive information or other commercial suppliers which are unfamiliar with government contracting.

C. Broader Requirements for Overseas Contracts Valued over $500,000

The CTIP FAR clause includes commitments to have a compliance plan for prevention, monitoring and detection of trafficking in persons, to include engaging in due diligence to determine potential violations in the contractor's supply chain and obtaining certifications of no violations in the supply chain. All of which apply only to contracts and subcontracts (except COTS) where the estimated value of the supplies to be acquired, or services required to be performed, outside of the United States exceeds $500,000. The CTIP rules state that the compliance plan must be appropriate (1) to the size and complexity of the contract; and (2) to the nature and scope of the activities to be performed under the contract, including the number of non-US citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking.

Although the final rule identifies certain minimum elements for this compliance plan (identified at FAR 52.222-50(h)(3)), the discussion in the regulatory history of the CTIP rules makes it clear that the compliance plan is not a one-size-fits-all commitment:

> The prime contractor's monitoring efforts will vary based on the risk of trafficking in persons related to the particular product or service being acquired and whether the contractor has direct access to a work site or not. Where a prime contractor has direct access, the prime contractor would be expected to look for signs of trafficking in persons at the workplace, and if housing is provided, inspect the housing conditions. For cases where the employees and subcontractors are distant, or for lower tier subcontractors, the prime contractor must review the plans and certifications of its subcontractors to ensure they include adequate monitoring procedures, and to compare this information to public audits and other trafficking in persons data available.

80 Fed. Reg. 4967, 4976 (Jan. 29, 2015). Importantly, these minimum commitments must be flowed down to all subcontracts and contracts with agents, except that, the compliance plan commitment applies only to non-COTS, overseas subcontracts for which the overseas portion exceeds $500,000.

Like other areas of supply chain compliance, the CTIP rules speak to conducting due diligence reviews of contractors' supply chains. In the case of the CTIP rules, for overseas contracts and subcontracts valued at greater than $500,000, contractors (and subcontractors) undertake to conduct due diligence and investigate whether their agents and subcontractors have engaged in prohibited practices before certifying compliance to the Government. In addition to certifying that the contractor maintains a CTIP compliance plan, the contractor commits to making one of the following certifications to the CO annually after receiving an award and "[a]fter having conducted due diligence:"

> (A) To the best of the Contractor's knowledge and belief, neither it nor any of its agents, subcontractors, or their agents is engaged in any such activities; or
>
> (B) If abuses relating to any of the prohibited activities identified in [the policy] of this clause have been found, the Contractor or subcontractor has taken the appropriate remedial and referral actions.

80 Fed. Reg. 4967, 4992.

Thus, the CTIP rules incentivize companies to engage in risk assessment and due diligence prior to and during contract performance. Similarly, to comply fully with CTIP rules and have an effective due diligence and risk assessment program to combat trafficking in persons, contractors will likely need to implement effective training, monitoring, auditing, and reporting systems.

D. 2016 Update

1. Regulatory Developments

The FAR Council's 2015 CTIP rules left unresolved a critical definitional issue that impacts the breadth of the new FAR policy prohibiting companies from charging employees or potential employees any "recruitment fees." In May 2016, the FAR Council sought to resolve that issue by publishing a proposed definition of "recruitment fees." The proposed definition is drafted very broadly and includes virtually any cost associated with "soliciting, identifying, considering, interviewing, referring, retaining, transferring, selecting, testing, training, providing new-hire orientation, recommending, or placing employees or potential employees." The proposed definition also includes a lengthy list of additional circumstances and types of costs that may not be passed on to employees or potential employees. After the submission of comments on the proposed definition on July 11, 2016, contractors should look for a resolution of the breadth of prohibited employee paid "recruitment fees" issue in the near future.

2. CTIP Compliance Resources

In May 2016, the US Department of State sponsored an on-line resource tool for combating trafficking in persons in US Government contractors' supply chains. The website, responsiblesourcingtool.org, contains a sample CTIP compliance plan, tools for assessing the risk posed by different aspects of contract performance (including place of performance, types of labor used, and products being sourced), links to additional CTIP compliance resources, and a wide variety of case studies and data to aid contractors in enhancing their CTIP compliance

processes. Because the groups that created the website's content partnered with the Department of State, and because the content will be periodically updated with new information on risk assessments and other tools, the site should provide government contractors with a reliable starting point for CTIP compliance information.

XIII. Government Contracts Intellectual Property

There is a well-developed framework for allocating rights in intellectual property between the Government and its prime contractors. This is reflected in regulations and contract clauses relating to rights in non-commercial and commercial technical data and computer software and in clauses allocating patent rights. Those provisions can have important impacts on prime/subcontractor relationships.

A. Technical Data and Computer Software

As a general rule, when dealing with intellectual property, the Government, with certain exceptions, purchases license rights, rather than full title. This reflects the policy that the Government should purchase only what it needs (i.e., rights defined in licenses) rather than full ownership rights (which will cost taxpayers more).

These license rights are found in both the Federal Acquisition Regulation (FAR), which applies to civilian government agencies, and the Defense FAR Supplement (DFARS), which applies to DoD agencies. (This is one of the rare instances in which the DFARS supplants, rather than supplements, the FAR.)

Under DFARS sections 252.227-7013 and 7014, rights in non-commercial technical data and computer software are generally allocated through different categories of license rights granted by the contractor to the Government – which are called unlimited rights, or limited rights (for technical data) or restricted rights or government purpose license (GPL) rights (for computer software). The rights that the Government obtains will generally depend on the source of funding (exclusively at government expense, exclusively at private expense or with mixed funding, respectively). FAR 27.401 similarly defines limited and unlimited/restricted rights data/computer software based on the source of funding, though it does not provide for GPL rights. Under FAR 27.404-1, the Government, with certain exceptions, acquires unlimited rights in "[d]ata first produced in the performance of a contract," and "[a]ll other data delivered under the contract other than limited rights data or restricted computer software." The contractor usually retains ownership, as well as all rights in technical data or computer software that are not granted to the Government by the contractual license. *See* DFARS 227.7103-4(a); 227.7203-4(a); FAR 52.227-14(b)(2).

Protection of rights in technical data and computer software is subject to a number of procedural requirements. For example, the DFARS contains a "pre-notification" provision, which requires the contractor to identify noncommercial technical data or computer software that the contractor (or its subcontractors) will deliver with restrictions on the Government's use, release or disclosure (i.e., with less than unlimited rights). *See* DFARS 227.7103-3(b); 227.7103-10(a); 227.7203-3; 227.7203-10(a); DFARS 252.227-7017. FAR 52.227-15 permits inclusion of a similar clause that provides for pre-award identification of technical data or software to be delivered with limited or restricted rights.

Technical data and computer software for which the Government receives less than unlimited rights also should be marked with an appropriate restrictive legend describing the rights which the Government obtains. The prescribed legends are set out in FAR 52.227-14(g)

(Alt. II or Alt. III) and DFARS 252.227-7013(f) and 252.227-7014(f). These requirements are critical: failure to provide a required pre-notification or to include the appropriate restrictive legend may waive protection of the contractor's rights in data or software, and result in the Government's obtaining greater rights in the data or software than were intended or justified under FAR 27.404-5(i); 227.7103-10(c); 227.7203-10(c). DoD contractors (and their subcontractors) are required to have written procedures for ensuring appropriate use of restrictive legends and to maintain documentation sufficient to justify the validity of claimed restrictions on the Government's right to use or disclose data or software under DFARS 227.7103-11, 227.7203-11, 252.227-7013(g), 252.227-7014(g), 252.227-7019(b) and 252.227-7037(c).

The Government can also include contract clauses that permit it to defer ordering or delivery of technical data or computer software for various periods after acceptance, per DFARS 227.7103-8, 227.7203-8, 252.227-7026 (delivery) and 252.227-7027 (ordering). Deferred ordering or delivery also extends to subcontractor data or software. Similar, but not identical, provisions in FAR 27.406-2(b) and 52.227-16 permit deferred ordering by civilian agencies.

Consistent with government procurement policy, purchase of commercial software or data is less encumbered by government rights and restrictions. For "commercial items," DFARS sections 227.7102-1 and 252.227-7015 specify that DoD agencies are to obtain only technical data that is customarily provided to the public with such items, although there are some limited exceptions, e.g., form, fit or function data, and data required for repair, installation or maintenance. Similar policies apply to commercial computer software where the Government acquires commercial computer software or software documentation under the same license rights customarily granted to the public, provided those licenses are consistent with federal law and satisfy the Government's needs. Some terms commonly found in standard commercial software licenses, such as indemnity, choice of law and disputes provisions, may be inconsistent with federal law. *See* DFARS 227.7202-1(c); 227.7202-3. Technical data related to commercial items should be properly marked, however, or else the Government can assert an unrestricted right to use or disclose the data. DFARS 227.7102 -3 & 4(c); 252.227-7015(b)(1)(i), (d).

The FAR coverage for technical data for commercial items and commercial computer software is similar to that prescribed in the DFARS. For example, FAR 12.211 limits the Government to acquiring "only the technical data and the rights in that data customarily provided to the public with a commercial item or process," and includes a presumption that any "data delivered under a contract for commercial items was developed exclusively at private expense." This presumption reinforces the commercial item contractor's right to provide commercial data and software with limited or restricted rights. Likewise, commercial computer software or commercial computer software documentation is to be "acquired under licenses customarily provided to the public to the extent such licenses are consistent with Federal law and otherwise satisfy the Government's needs" under FAR 12.212 and 27.405-3. The FAR also permits use of a Commercial Computer Software License clause, 52.227-19, although its terms can be problematical because they are not necessarily consistent with commercial license terms

B. Technical Data and Computer Software: Subcontracts

The DFARS expressly provides for the mandatory flow down to subcontractors of a number of contract clauses pertaining to technical data and computer software, including, for

example, the basic rights in non-commercial data and computer software clauses, and clauses relating to the Government's right to challenge restrictive markings. DFARS 227.7103-15(c); 227.7203-15(c); 252.227-7013(k) & 7014(k), 7019(i) (Validation of asserted restrictions – Computer Software), & 7037 (Validation of restrictive markings on technical data). Important other clauses – for example, those relating to deferred delivery or deferred ordering – are not specifically required to be flowed down by the FAR, but as a practical matter may need to be flowed down in order for a prime contractor to comply with its obligations to the Government.

In addition to the Government's rights, the prime contractor may seek rights in order to ensure successful contract performance. Ownership of and license to data and computer software is sometimes a bone of contention between prime contractors (which may seek rights that go beyond what is required to perform the prime contract) and subcontractors (which may be reluctant to provide data and software ownership or license rights to a prime contractor that may be a competitor in other programs). The DFARS has some specific language that can protect subcontractors in this battle. Specifically, the DFARS contract clauses, 252.227-7013(k) and 7014(k), preclude prime contractors from using the award of a subcontract as leverage to obtain rights in subcontractor data, or to modify the clauses to enlarge their rights in subcontractor data. Even though prime contractors should not normally require ownership rights in their subcontractors' non-commercial data or software, they may still need to obtain license agreements in cases where the prime contractor needs to use subcontractor data or software in performance of the prime contract.

The Government also is precluded from requiring contractors to have subcontractors relinquish rights in data or software (other than rights provided under applicable clauses) to the contractor (or higher-tier subcontractor), or to the Government, as a condition for award of a subcontract per DFARS 227.7103-15(d) and 227.7203-15(d).

As noted above, both prime contractor and subcontractor technical data and computer software should be properly marked to effectuate limitations on the Government's rights, and DFARS 252.227-7013(k)(1) and 7014(k)(3) impose an obligation on prime contractors to ensure that subcontractor rights are adequately protected in the identification, assertion and delivery processes. *See also* DFARS 252.227-7017(c). Although communications with the Government relating to contract administration are generally by and through the prime contractor, DFARS 227.7103-15 and 227.7203-15 permits the Government to communicate directly with the subcontractors with respect to validation of or challenges to restrictive markings on subcontractor technical data or computer software, albeit without creating privity of contract. Subcontractors also can submit technical data with other than unlimited rights directly to the Government, rather than through the prime contractor. DFARS 252.227-7013(k)(3).

In contrast to the DFARS, the FAR does not require flow down of the FAR data rights clauses and does not contain the same protection of subcontractor data rights vis-à-vis the prime contractor. However, the FAR does require prime contractors to obtain from subcontractors all data and rights necessary for the prime contractor to fulfill its obligations under the prime contract. FAR 52.227-14(h). If a subcontractor refuses to accept terms affording the Government those rights, the FAR clause directs the prime contractor to notify the contracting officer and prohibits the prime contractor from proceeding with award of the subcontract without authorization from the contracting officer.

Prime contractors holding contracts that include the DFARS clause at 252.227-7015, "Technical Data – Commercial Items" are required to include that clause in subcontracts under their prime contracts where technical data will be obtained from the subcontractor for delivery to the Government. DFARS 227.7102-3(a). There is no mandatory flow down requirement for the FAR clause at 52.227-19, "Commercial Computer Software – Restricted Rights." Prime contractors should ensure that the Government can and will be bound by applicable subcontractor commercial licenses (except to the extent such terms are inconsistent with federal law).

C. Patent Rights

Under the standard Patent Rights clauses (FAR 52.227-11 and DFARS 252.227-7038) which are to be used in contracts for research, development and experimental work, the contractor has the right to elect to retain title to each "subject invention." A "subject invention" is any invention of the Contractor "made" (conceived or first actually reduced to practice) in the performance of work under the contract. The Government receives "a nonexclusive, nontransferable, irrevocable, paid-up license to practice, or have practiced for or on its behalf, the subject invention throughout the world," as well as march-in rights to grant a license to a third party if the contractor fails to take steps to achieve practical application of the invention. Some agencies, such as DOE and NASA, have patent rights clauses that can provide for a different allocation of rights in subject inventions.

The standard FAR and DFARS Patent Rights clauses include numerous procedural requirements, including disclosure of subject inventions to the CO; election to retain title to subject inventions, and filing of patent applications in subject inventions in which the contractor has elected to retain rights. As is the case with software and data, failure to properly disclose an invention or elect to retain patent rights within the prescribed times can result in loss of rights by the contractor.

D. Patent Rights: Subcontracts

The DFARS Patent Rights clause, 252.227-7038(*l*), generally provides for mandatory flow down to subcontractors, although the clause is to be modified to "retain all references to the Government and shall provide to the subcontractor all the rights and obligations provided to the Contractor in the clause." It also prohibits the prime contractor from obtaining rights in subcontractor subject inventions as part of the consideration for the award of a subcontract. In addition, in a rather unusual provision, the clause provides that the parties (agency, the subcontractor, and the contractor) agree that the clause creates "a contract between the subcontractor and the Government with respect to those matters covered by this clause," except that there is no jurisdiction under the Contract Disputes Act to challenge the Government's march-in rights with respect to inventions. The FAR Patent Rights clause is essentially the same in this regard.

E. Authorization and Consent

In commercial disputes an aggrieved patent or copyright holder may seek to enjoin infringement by a commercial entity. In contrast, by statute, the Government is not subject to

injunctive relief. 28 U.S.C. § 1498 (Patent and copyright cases). Instead, an aggrieved patent or copyright holder is limited to a suit against the United States for royalties, which can be extremely time consuming and expensive to bring.

This limitation on injunctive relief may extend to government contractors and subcontractors when they act with the Government's "authorization and consent" and the appropriate clauses are included in the contract and subcontract. FAR 52.227-1 (Authorization and Consent) provides this protection from injunctive relief to any invention covered by a patent that is "embodied in the structure or composition of any article . . . accepted by the Government," or "used in machinery, tools, or methods" resulting from compliance by the contractor or subcontractor with contract specifications or provisions or written instructions from the Contracting officer. An alternative version (Alt I), which is used mainly in research and development contracts, is even stronger, and extends to "all use and manufacture of any invention described in and covered by a United States patent in the performance of this contract or any subcontract at any tier." These clauses are to be flowed down to subcontractors. Although the FAR clause is limited to patent rights, the underlying federal statute applies to copyright actions as well.

This potential protection for contractors from injunctive relief is important. Most importantly, if a contractor is acting with the Government's "authorization and consent," it is very unlikely that contract performance may be stymied by a badly-timed injunction from an unfriendly court. In addition, the contractor (and subcontractor) would not have to incur the costs of litigating a patent or copyright infringement claim. This latter protection is not total, however, because if an aggrieved patent or copyright holder sues the Government for royalties, the contractor (or possibly the subcontractor) may be required to indemnify the Government if the contract includes FAR 52.227-3 (Patent Indemnity). This risk is usually low, however; royalty actions against the United States are infrequent because they are generally extremely time-consuming and expensive to bring.

F. Other Potential IP Issues

Many other IP issues can arise in the supply chain context, but are outside the scope of this discussion. These include proper marking of proposal information, copyrights, protection of technical data and computer software provided to government support contractors, and protection of proprietary and confidential business information from disclosure pursuant to Freedom of Information Act requests.

XIV. Contracting with Small Businesses

It is the policy of the United States to provide "maximum practicable opportunit[ies]" for small businesses to compete for and obtain award of federal prime contracts as well as subcontracts awarded in the performance of federal contracts. 15 U.S.C. § 637(d)(1). Accordingly, contracting officers are directed to consider setting aside procurements for the exclusive participation of small business. FAR Subpart 19.5. Large businesses also are required to implement subcontracting plans to identify "maximum practicable subcontracting opportunities for small business concerns" in the performance of federal contracts. 13 C.F.R. § 125.3; FAR Subpart 19.7.

There are a number of compliance-related risks for any entity seeking to take advantage of programs designed to benefit small businesses in federal procurement. Because this Toolkit focuses on supply chain risks, it does not address all of those risks but instead discusses three potential risks when contracting with small businesses in the performance of a federal contract, where the small business is performing work as the prime contractor or the subcontractor.

A. Maintaining the Role of the Small Business as the Prime Contractor

Because many federal procurements are set aside exclusively or partially for contract award to a small business (or provide price preferences to certain small businesses), large companies may consider pursuing subcontracting opportunities with small business prime contractors to obtain a portion of those federal dollars. Although there is no prohibition against a large business serving as a subcontractor on such contracts, there are restrictions on the role of the large business in both the contract and the affairs of the small business. These restrictions should be considered to preserve the prime contractor's eligibility for a set-aside award as well as its small business status.

On May 31, 2016, the Small Business Administration (SBA) adopted a final rule that amended its "Limitations on Subcontracting" regulations to implement provisions of Section 1651 of the FY 2013 National Defense Authorization Act. Previously, the regulations established a minimum percentage of work that a small business prime contractor must perform in a set-aside contract, using different measurements that depended on the type of contract and, in some cases, the socioeconomic status of the small business. Under those regulations, the small business prime contractor's direct labor costs were calculated as a percentage of the total direct labor costs for the contract, and the contractor was deemed to have satisfied the minimum level of work requirement if the calculated percentage met a certain threshold based on the contract type.

The final rule, effective June 30, 2016, removes the direct labor cost calculation to determine compliance. Instead, for full or partial set aside contracts with a value greater than $150,000, the revised regulations limit the subcontracting amount to a percentage of the award amount received by the small business prime contractor. *See* 13 C.F.R. § 125.6(a), (f). For example, the limitation or cap on subcontracting for both services contracts and supplies contracts is set at 50% of the award amount received by the small business prime contractor. *See* 13 C.F.R. § 125.6(a)(1)-(2). The limitation or cap for general construction subcontractors is 85% of the award amount (75% if the contract is for "special trade" subcontractors). *See* 13 C.F.R.

§ 125.6(a)(3)-(4). A different set of rules applies to contracts for both services and supplies (i.e., "mixed contracts"). *See* 13 C.F.R. § 125.6(b).

Unrelated to the SBA's rules, some fixed-price construction contracts may include the FAR's "Performance of Work" clause (52.236-1), which requires the prime contractor to perform "with its own organization" a certain percentage of the total amount of work to be performed under the contract, which identified on a contract-by-contract basis by the agency. This clause, however, should not be used in procurements set aside for small businesses. *See* FAR 36.501(b).

To facilitate small businesses to work together (in competing against larger firms), the regulations exclude the amounts paid to "similarly situated" firms from the limitation on subcontracting calculation for the types of contracts identified in FAR Part 52.219-14. *See* 13 C.F.R. § 125.6(a)(1), (2), (3), (4); 13 C.F.R. § 125.6(c). The revised regulations provide that work performed by a similarly situated firm is not deemed to be subcontracted and will not be included in the determination of whether the small business prime contractor has complied with the limitations on subcontracting provision. *See* 13 C.F.R. § 125.6(c). An entity is a similarly situated subcontractor if it is a participant of the same size or socioeconomic category that qualified the prime contractor as the contract awardee. The work subcontracted to a similarly situated firm will count as work performed by the small business prime contractor; however, any work subcontracted by the first-tier similarly situated subcontractor will be counted as subcontracting to a non-similarly situated firm. The exclusion of similarly situated entities from the limitations on subcontracting calculation is viewed as consistent with the Government's policy of promoting opportunities for small business concerns.

Compliance with the applicable limitations on subcontracting, however, does not inoculate the small business from potential scrutiny under the SBA's rules on affiliation. In assessing a firm's size under the SBA's size standards, the SBA considers the size of any firms "affiliated" with the firm claiming "small business" status. In general, the SBA's regulations provide that two businesses are affiliates of each other when one controls or has the power to control the other, or a third party controls or has the power to control both. 13 C.F.R. § 121.103(a). In assessing affiliation, those rules identify a number of broad factors that could be implicated even by arms-length subcontracting relationships, such as contractual relationships, identity of business or economic interests, or economic dependency through contractual or other relationships. 13 C.F.R. § 121.103(a), (f).

In 2016, the SBA adopted a rule to clarify the type of relationships between individuals that create a rebuttable presumption of affiliation due to an identity of interest. 13 C.F.R. § 121.103(f)(1). The clarifying language identifies firms owned or controlled by "married couples, parties to a civil union, parents, children, and siblings" as presumed to be affiliated if they conduct business with each other either as subcontractors or joint venturers, or share or provide loans, resources, equipment, locations or employees. 13 C.F.R. § 121.103(f)(1). The SBA also adopted a presumption of affiliation based on a fixed percentage of economic dependence of one firm on another. 13 C.F.R. § 121.103(f)(2). Specifically, the SBA will find a presumption of affiliation if a firm derives 70% or more of its revenue from another firm. The presumption of affiliation is rebuttable and economic dependence is measured over a three year period.

The SBA also applies an "ostensible subcontractor" rule, providing for a potential finding of affiliation where a subcontractor performs "primary and vital" requirements of a prime set-aside contract or where the small prime contractor is "unusually reliant" on a large subcontractor. 13 C.F.R. § 121.103(h)(4). If the SBA determines that two entities are affiliated under these rules, then the SBA considers the size of both entities for purposes of its size determination. In other words, a finding of affiliation with a large business means that the small business is not considered small. The 2016 revised rule also excludes "similarly situated subcontractors" from the application of the "ostensible subcontractor" rule. *Id*.; *see also* 13 C.F.R. § 125.6(c).

Although not every non-compliance with limitations on subcontracting or finding of affiliation would warrant enforcement activity by the Government, there could be severe consequences for failing to comply with these provisions, especially if the non-compliance is perceived as an effort by the large business to improperly benefit from programs designed to support small businesses. Those consequences could range from the termination of the contract, the pursuit of civil or criminal remedies including penalties and fines under the Small Business Act, the False Claims Act, and Program Fraud Civil Remedies Act, or the suspension or debarment from government contracting. Congress, for example, amended the Small Business Act to provide that "[w]hoever violates" one of the enumerated limitations on subcontracting would be subject to the penalties of $500,000 or the amount spent on large subcontractors in excess of the limitations, whichever is greater, in addition to other remedies, such as suspension or debarment. 15 U.S.C § 645(d) & (g); 13 C.F.R. § 125.6(h). Similarly, in an effort to overcome certain obstacles faced by the Government in proving actual damages caused by the successful performance of a contract awarded to a firm misrepresenting its size status, Congress has attempted to implement a presumption of loss to the Government equal to the total amount the Government expended on the contract. 15 U.S.C. § 632(w); 13 C.F.R. § 121.108(a).

To manage supply chain risks in performing a contract set aside for small businesses, both the small and large contractors should be cognizant of the applicable regulations and contract terms limiting the role of large businesses in the performance of small business set-aside contracts and consider taking steps to ensure that the prime-subcontractor relationship is documented and could withstand scrutiny. For example, a small business seeking to subcontract with a large business should monitor and audit its own size eligibility before representing itself as eligible. Both contractors also could consider documenting (i) how the relationship meets the precise calculation identified in the Limitation on Subcontracting clause (and any other "performance of work" requirements applicable to the small business prime contractor) and (ii) how the relationship is consistent with the SBA's affiliation rules.

B. Joint Ventures with Small Businesses under the All Small Mentor-Protégé Program: Maintaining the Role of the Protégé

In 2016, the SBA also issued regulations to implement authority to establish mentor-protégé programs for all small businesses – authority that had been granted by the Small Business Jobs Act of 2010 and the National Defense Authorization Act for Fiscal Year 2013. Prior to the implementation of the regulations, the mentor-protégé program had been limited to participants qualifying under the SBA's 8(a) program (for small businesses owned or controlled by socially and economically disadvantaged individuals). Under the new regulations, the SBA maintain the 8(a) program and created another mentor-protégé program for all small businesses,

which is modeled on the 8(a) program and available to women-owned small business (WOSB), service-disabled, veteran-owned small business (SDVOSB), HUBZone concerns, and small businesses that are not part of a designated SBA program. The SBA dubbed it the "All Small Mentor-Protégé Program."

The program encourages approved mentor firms to provide business development assistance to protégé firms and to help protégé firms successfully compete for government contracts. 13 C.F.R. § 125.9(a). The regulation permits the mentor to provide a broad range of assistance to the protégé, including technical and/or management assistance, financial assistance (equity investments and/or loans), subcontracting (either with the mentor as the prime contractor or subcontractor), trade education, or performing federal contracts as the prime contractor through joint venture arrangements. In addition, the rules encourage mentors to provide assistance relating to the performance of contracts set aside or reserved for small business so that the protégé may fully develop its capabilities.

To qualify as a mentor, the contractor must demonstrate a commitment and ability to assist small businesses, possess good character, and cannot be a debarred or suspended contractor. 13 C.F.R. § 125.9(b). The SBA also will evaluate the prospective mentor's financial capability, including consideration of tax returns, audited financial statements, and SEC filings. 13 C.F.R. § 125.9(b)(2). After the contractor is approved as a mentor, it must annually certify that it continues to possess good character and favorable financial capabilities. 13 C.F.R. § 125.9(b)(3). With the SBA's authorization, a mentor may have more than one protégé, but no mentor will be permitted to have more than three protégés at one time (inclusive of protégés under the All-Small program and the existing 8(a) program). 13 C.F.R. § 125.9(b)(4).

To qualify as a protégé, the concern must "qualify as small for the size standard corresponding to its primary NAICS code or identify that it is seeking business development assistance with respect to a secondary NAICS code and qualify as small for the size standard corresponding to that NAICS code." 13 C.F.R. § 125.9(c)(1). If the prospective protégé is not small in its primary NAICS code and it seeks to qualify as small under a secondary NAICS code, it must demonstrate how the mentor-protégé relationship is a logical business progression that would further develop the firm's capabilities. The SBA will not approve a mentor-protégé relationship for a secondary NAICS code in which the firm has no prior experience. With the SBA's approval, a protégé may have more than one mentor, but it may not have more than two concurrent mentors.

The rule allows mentors to own up to 40% of the small business protégés. 13 C.F.R. § 125.9(d)(iii)(B)(2). All mentor-protégé relationships must be formalized in a written agreement that identifies the protégé's needs and provides a detailed description of the mentor's commitment to meet those needs for at least one year. 13 C.F.R. § 125.9(e). Agreements are limited to an initial term of three years, but the SBA will authorize and extend an additional three year term provided that the protégé has received and will continue to receive the agreed-upon business development assistance. The SBA must review and approve the written agreement before it takes effect and the SBA must approve all changes to the written agreement. 13 C.F.R. § 125.9(e)(6). The SBA's control and affiliation rules will not automatically apply based solely on an approved mentor-protégé agreement, but compliance with the affiliation rules, as set forth in 13 C.F.R. § 103, is still generally required. 13 C.F.R. § 125.9(d)(4).

The new rules also require the protégé to provide an annual report to the SBA and provide a narrative that describes the success achieved in meeting the protégé's developmental needs. 13 C.F.R. § 125.9(g). After the relationship has concluded, the protégé must submit a final report to the SBA that addresses whether the relationship was beneficial. 13 C.F.R. § 125.9(i).

For "other than small" contractors, the most significant aspect of this new program is that it permits the mentor and protégé – once approved by the SBA – to form a joint venture that would be treated as a small business for any type of prime contract or subcontract for which the protégé qualifies as small. 13 C.F.R. § 125.9(d)(1). Under the rules, the mentor-protégé may enter into this second agreement to form a joint venture, but those agreements must be in writing and also approved by the SBA before the joint venture submits an offer on a prime contract or subcontract, in order to receive an exclusion from the SBA's affiliation rules. 13 C.F.R. § 125.9(d)(1)(1)(ii).

Although the affiliation rules would not apply based solely on the mentor-protégé relationship, the joint venture must still comply with 13 C.F.R. § 125.8(b)(2), (c), (d). Among other things, those rules require the joint venture agreement to identify the specific tasks assigned to each member of the joint venture (including major equipment, labor, and other resources). *See* 13 C.F.R. § 125.8(b)(2). The joint venture also must satisfy the applicable percentage of work requirement set forth in 13 C.F.R. §125.6 for the type of work being performed by the joint venture combined and the protégé of the joint venture must perform at least 40% of the substantive work performed by the joint venture. 13 C.F.R. § 125.8(c). Finally, the joint venture must submit written certification to the contracting officer and the SBA stating that the parties have entered into a joint venture that complies with Sections 125.8(b)(2) and 125.8(c) before performing the contract. 13 C.F.R. § 125.8(d).

Many of the same compliance-related risks apply to both the mentor and protégé seeking to take advantage of this expanded program. If the SBA determines that the mentor failed to provide the protégé with the assistance that it committed to provide under the agreement and the mentor fails to provide an adequate explanation for the failure, the SBA may terminate the agreement. Among other remedies, the SBA may declare the mentor ineligible to act as a mentor for a period of two years, recommend that the procuring agency issue a stop work order on all federal contracts that the mentor and protégé are performing as a small business, and refer the mentor for potential suspension and debarment. 13 C.F.R. § 125.9(h). The SBA also will evaluate compliance based on any mentor-protégé joint ventures that fail to comply with 13 C.F.R. §§ 125.8(b)(2), (c), (d), (g) and will consider the same types of remedies listed above as well as potential remedies under available fraud statutes, such as the civil False Claims Act.

C. Small Business Subcontracting Plans for Large Businesses

Where the large business is the prime contractor in an unrestricted procurement, FAR 52.219-9 requires large business contractors to prepare and comply with subcontracting plans for federal contracts or subcontracts for goods and services exceeding $700,000 (or $1,500,000 for construction contracts). Subcontracting plans set forth a commitment by the large business identifying its goals for contracting with small businesses (to provide "maximum practicable opportunities"), including goals by each socioeconomic category, such as those owned or

controlled by veterans, service disabled veterans, women, or socially and economically disadvantaged individuals, and its plan for meeting those goals. Large contractors are generally held accountable to achieve, or make good faith efforts to achieve, the written goals established in their subcontracting plans.

Contractors are not required to prepare and to submit subcontracting plans where (1) the prime contractor is a small business or small disadvantaged business; (2) the contract is a personal services contract; or (3) the contract will be performed entirely outside of the United States. There is also an exception for contracts including FAR 52.212-5 (contracts for commercial items). FAR 52.219-9 (d)(9) further provides for the prime contractor to flow down the requirement for a small business subcontracting plan to "all subcontractors (except small business concerns) that receive subcontracts" in excess of the dollar thresholds above where there is "further subcontracting possibilities."

There are three types of subcontracting plans: (1) commercial plans; (2) individual plans; and (3) master plans. *See* FAR 19.701, 19.704. Commercial subcontracting plans are company-wide plans that contain goals based on the contractor's planned subcontracting for all of its business. FAR 19.704(d). Commercial plans are preferred for contractors that furnish commercial products or services to the Government and to commercial customers and are negotiated and submitted annually based on the company's fiscal year.

An individual subcontracting plan applies to a specific contract and covers the entire contract period, including option periods. The goals for individual plans are based on the contractor's planned subcontracting in support of the specific contract, stated in terms of separate dollar and percentage goals. Individual plans must be negotiated and approved by the contracting officer prior to award.

Master subcontracting plans contain all of the required elements of an individual plan, except goals. FAR 19.704(b). Master plans are then supplemented by individual contract goals when contracts are awarded. Master plans are in effect for three years; however, master plans will apply to a contract for the life of the contract when the master plan is incorporated into an individual plan.

Each subcontracting plan should contain the following eleven required elements, as provided in FAR 19.704(a):

1. Separate percentage goals for using small businesses by socioeconomic category.

2. A statement of the total dollars planned to be subcontracted and a statement of the total dollars planned to be subcontracted to small businesses.

3. A description of the principal types of supplies and services to be subcontracted and an identification of types planned for subcontracting to each group, including other than small business subcontractors.

4. A description of the method used to develop the subcontracting goals.

5. A description of the method used to identify potential sources for solicitation purposes.

6. A statement as to whether indirect costs were included in the subcontracting goals; and if so, a description of the method used to determine the proportionate share of indirect costs to be incurred with small business.

7. The name of the administrator of the subcontracting plan and a description of the duties of the individual.

8. A description of the efforts the contractor will make to ensure that small businesses have an equitable opportunity to compete for subcontracts.

9. Assurances that the contractor will include the clause at FAR 52.219-8, "Utilization of Small Business Concerns," in all subcontracts that offer further subcontracting opportunities, and that the contractor will require all subcontractors that receive subcontracts in excess of $700,000 to adopt a plan that complies with the requirements of FAR 52.219-9, Small Business Subcontracting Plan.

10. Assurances that the contractor will cooperate in any studies or surveys as may be required; the contractor will submit periodic reports to allow the Government to determine the extent of compliance by the contractor with the subcontracting plan; and the contractor agrees to submit required reports, including the Individual Subcontract Report (ISR), and the Summary Subcontract Report (SSR) using the Electronic Subcontracting Reporting System (eSRS).

11. A description of the types of records that the contractor will maintain to demonstrate its compliance with the subcontracting plan.

The revised SBA regulations also require prime contractors to provide prior written notice to a subcontractor that it intends to identify the small business by name as a potential subcontractor in a proposal, offer, bid or subcontracting plan in connection with a federal contract. 13 C.F.R. § 125.3(c)(8).

As indicated in item number 10 above, to assess the extent of compliance with the subcontracting plan, contractors are asked to submit "timely and accurate" subcontracting reports (semi-annually for DoD and NASA) that set forth their status, achievements, and compliance with the plan's goals. 13 C.F.R. § 125.3(c)(vi); *see also* FAR 52.219-9. In making these statements about compliance and subcontracting with small businesses, the FAR provides that "[a] contractor acting in good faith may rely on the written representation of its subcontractor regarding the subcontractor's status as a small business" and its socioeconomic status. FAR 19.703(b). In 2016, the SBA adopted regulations that require the contracting agency to collect, report, and review data on the extent to which the large contractor complies in good faith with the goals and objectives of its subcontracting plan. 13 C.F.R. § 125.3(f)(8). The revisions also impose reporting requirements for anyone who believes that a prime contractor or subcontractor has engaged in fraudulent activity or bad faith behavior related to its subcontracting plan. 13 C.F.R. § 125.3(c)(9).

The SBA regulations similarly provide that "[a] prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' size." 13 C.F.R. § 121.108(d). This regulation further states that "[r]elevant factors to consider" in evaluating the prime contractor's good faith "may include the firm's internal management procedures governing size representation or certification, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner." *Id*. These provisions are repeated for various socioeconomic small business categories at 13 C.F.R. §§ 121.411(h), 124.521(d), 124.1015(d), 125.29(d), 126.900(d), and 127.700(d).

These SBA regulations suggest that, prior to seeking credit for subcontracting with a small business, a prime contractor may wish to consider taking some affirmative steps to document its "good faith." Depending on the particular facts and type of procurement, such steps could include maintaining written representations received from small businesses, checking those representations against data available in federal contracting databases, such as the System for Award Management at www.sam.gov (a step that a contractor must take for a subcontractor representing itself as a HUBZone small business under FAR 19.703(d)(1)), and asking vendors to update representations on an annual basis or due to a change in status. Contractors are not generally held liable for missing a goal, as long as they have made a good faith effort to reach that target and have followed their subcontracting plans in doing so. In evaluating whether a prime contractor made a good faith effort to comply with its small business subcontracting plan, contracting officers may consider, among other factors, supporting documentation showing that (1) the contractor performed the actions identified in the SBA's regulations for maximizing small business subcontracting opportunities, such as market research about available small businesses or soliciting offers from small businesses early in the procurement process; or (2) despite a contractor's failure "to achieve its goal in one socioeconomic category, it over-achieved its goal by an equal or greater amount in one or more of the other categories." 13 C.F.R. § 125.3(d)(3). Contractors also are subject to an on-site "compliance review" by the SBA, as a supplement to the contracting agency's review, to determine the "contractor's achievements in meeting the goals and other elements in its subcontracting plan for both open contracts and contracts completed during the previous twelve months." 13 C.F.R. § 125.3(f)(1).

If the prime contractor did not meet all of the small business subcontracting goals in its plan by contract completion, it will need to submit to the contracting officer a written explanation as to why it did not meet the plan's goals for the agency to evaluate whether the prime contractor acted in good faith in implementing its plan. 13 C.F.R. § 125.3(c)(6). A contractor's failure to make a good faith effort may result in a material breach of contract and termination for default. The contractor also is subject to the potential assessment of liquidated damages as provided under 13 C.F.R. § 125.3(f)(5)(i) and the procedures at FAR 19.705-7 and FAR 52.219-16. Those liquidated damages could equal to the actual dollar amount by which the contractor failed to achieve its subcontracting goals.

Regardless of the contractor's good faith efforts, the ramifications of a contractor's failure to meet the goals of its subcontracting plan can extend into the future. The 2016 revisions to the SBA regulations expressly state that a finding that a contractor failed to provide a written corrective action plan or failed to make a good faith effort to comply with the subcontractor plan will constitute a material breach of the contract and the failure will be considered in the past

performance evaluation of the contractor. 13 C.F.R. § 125.3(f)(5)(ii). This change is consistent with recent case law that has found that agencies are authorized to include an evaluation factor in a solicitation assessing the offeror's proposed approach to small business subcontracting, the extent to which it has met its small business subcontracting goals on previous covered contracts, and the extent to which it timely paid its small business subcontractors under covered contracts. 13 C.F.R. § 125.3(g). *See also Graybar*, B-410886, Mar. 4, 2015, 2015 CPD ¶ 102 (denying protest challenging exclusion from competitive range based on deficiencies under the past performance factor where offeror failed to include "the required information regarding socioeconomic subcontracting goals and actual performance in meeting its subcontracting plan goals"). As a result, to avoid missed goals and unfavorable evaluations in future procurements, contractors should consider various steps to increase the likelihood of success in implementing its plan. Such steps could include (1) appropriately defining the pool of dollars capable of being subcontracted to small businesses; (2) negotiating reasonable and realistic subcontracting goals based on the nature of the work; and (3) identifying in the plan discrete, objective steps for measuring good faith efforts for meeting the plan.

XV. Conclusion

As reflected in this Supply Chain Toolkit, the federal government has devoted a substantial amount of attention and effort to implement policies and regulations to address supply chain risks in procurement. Notwithstanding the change in administration in 2017, this trend will continue as we anticipate that the federal government will implement new and refined supply chain requirements focusing on areas critical to national security, international trade, and counterfeit parts. At the same time, to emphasize the importance of addressing these perceived risks, we also expect that there will be increased enforcement activities by the Government, ranging from noncompliance findings by contracting officers to the initiation of civil and criminal proceedings based on the alleged procurement of non-compliant goods and services. As a result, supply chain risk management should be a key element of a government contactor's internal compliance program.

Steptoe is available to work with clients in navigating these requirements, implementing risk management programs appropriate for a client's business, and, as necessary, responding to allegations of noncompliance with any supply chain requirements. For more information, please contact any one of the following Steptoe points of contact for government contracting supply chain risk management: Paul Hurst, Tom Barletta, Kendall Enyard, Andy Irwin, Sharon Larkin, Mike Mutek, Mike Navarre, and Fred Geldon (or visit Steptoe's Government Contracts Group website).