THOMSON REUTERS

BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

SUPPLY CHAIN RISK MANAGEMENT & COMPLIANCE

By Michael W. Mutek and Fred W. Geldon, Steptoe & Johnson LLP, and John F. Aylmer, Raytheon Company

In today's Government contracting environment, it is vital that companies understand the importance of supply chain risk management and compliance. What was historically thought of as "purchasing"—obtaining the right part, at the right time, at the right price—has evolved into a complex "supply chain" function. This function continues to be responsible for obtaining the right part (or service or license), at the right time, and at the right price, but its role has expanded. Today's Government contractor supply chain function must manage the risk associated with a globally dispersed network of suppliers and must address compliance with a broad range of laws and regulations.

A recent FORTUNE magazine interview with David Wilkins, vice president of contracts and supply chain at Raytheon Company, describes this change.[1] According to Wilkins, 20 or 25 years ago supply chain did not have "a voice at the table." Today, however, Wilkins' position reports directly to Raytheon's chief executive officer. As Wilkins notes: "We've gone from an organization where the vast majority of [supply chain] folks were…basically placing purchase orders…now we're

IN BRIEF

Michael Mutek and Fred Geldon are senior counsels in Steptoe & Johnson, LLP's Washington, D.C. office and members of the firm's government contracts practice group; John Aylmer is senior corporate counsel for supply chain in Raytheon Company's law department located in Waltham, Massachusetts. *The authors gratefully acknowledge the contributions by members of Steptoe's government contracts practice group in the preparation of this BRIEFING PAPER.*

  4-184-254-1

buying very complex systems. How we manage suppliers as they build those systems is really the value proposition that supply chain brings."[2] The metrics bear this out: where Raytheon once manufactured more than 80% of its products within its organization, today that percentage is closer to 30%.[3] This growing dependence on the supply chain—typical in this industry—increases the need and importance of effective supply chain risk management.

Supply chains are subject to a variety of laws, a growing list of supply chain regulations, and individual contract obligations. For Government contractors, supply chain management must include a compliance function that addresses (among other things) the requirements found in the Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS), many of whose provisions must be flowed down to suppliers. In addition, the FAR includes a framework for Government examination of a contractor's purchasing system (using an older term, "purchasing," rather than "supply chain"). This involves the Contractor Purchasing System Review (CPSR) used to evaluate supply chain risk and assess the contractor's effectiveness and efficiency in spending Government funds and complying with Government policy.[4]

This Briefing Paper begins by providing an overview of the evolution of supply chain management and then discusses (1) Government contractor supply chain risk management, (2) subcontractor selection, responsibility and past performance, (3) teaming and collaborative arrangements, (4) policies and procedures and standard forms and agreements, (5) supplier business ethics and conduct, (6) counterfeit parts, (7) cybersecurity, (8) intellectual property, (9) supply chains and socioeconomic considerations, (10) global supply chain issues, and (11) anticipated further regulation of the supply chain.

The Evolution Of Supply Chain Management

The evolution from a purchasing focus to a risk management and compliance focus demonstrates the growing importance of a company's supply chain function. Whether you are a contractor, subcontractor, or Contracting Officer (CO), work for an agency, or serve as legal adviser to a company or an agency, you are likely to be involved with supply chain issues. In this Briefing Paper we use the definition of subcontractor found in the FAR: "any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor or another subcontractor."[5]

Supply chain risk management and compliance issues can arise in all industries, but have heightened importance in a regulated industry such as Government contracting. Not only must the supply chain function ensure the contractor's (and subcontractors') compliance with laws, regulations, and policies, it must protect the interests of the customer—in this case, the interests of the U.S. Government. The Government has a vital interest in having a supply chain that can provide the nation, including its military, with needed goods and services, and to do so in a compliant manner. To achieve this goal, the Government expects its prime contractors and higher tier subcontractors to effectively police their supply chains.

THOMSON REUTERS

BRIEFING PAPERS

Briefing Papers® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2015 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.legalsolutions.thomsonreuters.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

A recent expression of the Government's concern can be found in the preamble to the final DFARS rule on "Requirements Relating to Supply Chain Risk," issued on October 30, 2015:[6]

> Congress has recognized a growing concern for risks to the supply chain for technology contracts supporting the Department of Defense (DoD). Congress has defined supply chain risk as the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

Many of the risks that Government contractors must effectively police are discussed later in this Briefing Paper. They include counterfeit parts, human trafficking, supplier business ethics, cyber threats, and restrictions relating to international trade. Government contractors must also comply with certain socioeconomic and domestic preference goals—all the while ensuring that goods and services meet quality requirements at competitive prices.

These trends are likely to continue. For example, the proposed "Fair Pay and Safe Workplaces" FAR rule includes a formidable requirement for contractors to collect supplier labor compliance information and review subcontractor responsibility.[7] Contractors need to seek advice regularly regarding changes in law and regulations and will need to consider necessary changes in their standard purchasing agreements, especially when new rules are issued on an interim basis, effective immediately without the benefit of a comment period. Similarly, their legal counsel will have to focus on supply chain issues as an important compliance area.[8]

The need for effective oversight of third parties has become more important—and more visible. For example, the 2014 Foreign Bribery Report issued by the Intergovernmental Organization for Economic Co-operation and Development (OECD) states that more than three-quarters of the 427 corruption cases analyzed involved misconduct by intermediaries.[9] The bottom line is that monitoring third-party compliance is not an option; it is a requirement for effective governance.

Globalization has increased Government customer concerns. For example, concern over counterfeit parts in the supply chain led to a DFARS rule (discussed in more detail below) that mandates the creation of procedures to monitor, detect, and eliminate counterfeit parts at all levels of the supply chain.[10] Noncompliance threatens an enterprise's ability to conduct business. A recent FAR rule seeking to eliminate trafficking in persons (also discussed further below) mandates the creation of procedures that include monitoring the supply chain.[11] And the final DFARS rule on "Requirements Relating to Supply Chain Risk," quoted above, reflects a concern over the risk of "back door" cyberattacks through a company's supply chain.[12]

Finally, mismanagement of supply chain risk can lead to a contractor's exclusion from programs and opportunities. The DFARS final rule on "Requirements for Information Relating to Supply Chain Risk" makes supply chain risk an evaluation factor and authorizes officials in the Department of Defense (DOD) to exclude sources from providing information technology on the basis of risk.[13] In addition, the Intelligence Community has 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."[14]

Government Contractor Supply Chain Risk Management

Although the Government's oversight of the contractor's supply chain function includes new rules, the framework for review has been around for some time.

■ Contractor Purchasing System Review

Where a contractor's "purchasing" exceeds the regulatory threshold, the Federal Government may decide to evaluate the contractor's purchasing system, including supply chain risks, using a Contractor Purchasing System Review (CPSR), conducted by the Defense Contract Management Agency (DCMA). A CPSR is "the complete evaluation of a contractor's purchasing of material and services, subcontracting, and subcontract management from development of the requirement through completion of subcontract performance."[15] The FAR states that the Administrative Contracting Officer (ACO) should determine whether to conduct a CPSR when a contractor's sales to the Government are expected to exceed $25 million during the next 12 months.[16] The purpose of the CPSR review is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy. It also provides the ACO with the basis for granting, withholding, or withdrawing approval of the contractor's purchasing system.[17]

In addition, a Government contractor's supply chain function, still called the "purchasing system," constitutes an important business system. Ever since the "business systems rule" was issued by the DOD in 2011,[18] a contractor must be concerned about the risk that one or more of its business systems may be deemed noncompliant due to a "significant deficiency."[19] In addition to mandatory penalties, a "significant deficiency" can increase the time and cost of contracting with the Government because it will require additional approvals and oversight.[20] The DFARS business systems rule lists 24 criteria that must be satisfied for a purchasing system to be deemed acceptable.[21] If the ACO deems that a purchasing system is significantly deficient in any one of these criteria, the system will be deemed "unacceptable."[22]

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 the contractor's purchasing files to determine whether those procedures have been followed. During the CPSR, special attention will be given to certain areas identified in the FAR, including:

(1) Market research;

(2) Degree of price competition;

(3) Pricing policies and techniques;

(4) Planning, award, and management of major subcontracts;

(5) Inclusion of appropriate flowdown clauses;

(6) Appropriateness of types of subcontracts used;

(7) 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;

(8) Policies and procedures pertaining to the small business subcontracting program;

(9) Treatment accorded affiliates and other concerns having close working arrangements with the contractor;

(10) Compliance with Cost Accounting Standards (CAS) (if applicable) in awarding subcontracts;

(11) Management control systems to administer progress payments; and

(12) Implementation of higher-level quality standards.[23]

The areas evaluated during the CPSR provide a useful checklist for all contractors. The development of policies and procedures to address these areas is an important step in the creation of a strong supply chain management system.

■ Purchasing System Approval

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. The Government, however, can play an important and sometimes burdensome role in supplier selection and in supplier oversight. The amount of this burden depends in large part on whether the contractor has an "approved" purchasing system.

A successful CPSR will result in "approval" of the contractor's purchasing system. This is important to the contractor's ability to conduct its business, because without an approved purchasing system the contractor will require the CO's consent to subcontract under cost-reimbursement, time-and-materials, labor-hour, or letter contracts, as well as unpriced actions under fixed-price contracts that exceed the simplified acquisition threshold. In situations where subcontractors must be added to the team on short notice, the need for CO consent can cause significant delay and disruption and can even jeopardize the contractor's ability to successfully perform the contract.

Where consent is required, the FAR lists several factors the CO must review and evaluate. These include the 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.[24]

■ Prime Contractor Risk Management Concerns

Because the supply chain activity serves a compliance function, contractors must develop processes to ensure compliance and identify risks. Risk management should serve as an early warning radar and be able to identify potential issues that could jeopardize the company's ability to meet its contractual obligations.

A contractor must first conduct due diligence in the selection of its suppliers and then actively police its supply chain during contract performance to avoid the risks of—

(1) Counterfeit parts;

(2) Human trafficking;

(3) Cybersecurity threats;

(4) Failure to meet socioeconomic and domestic preference goals;

(5) Disputes, claims, and litigation;

(6) Potential suspension or debarment of suppliers; and

(7) Reputational damage from having a bad actor in the supply chain.

Companies will 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 continue adequate oversight of the suppliers throughout performance.

You must also worry about becoming "hostage" to a poorly performing supplier. Where too much time has passed and it has become difficult to terminate the arrangement and locate a qualified alternative source, you may be forced to continue to work with the poor performer. This emphasizes the need for early and ongoing supplier audits and careful first article inspections. A best practice is to establish a supplier management plan before finalizing the subcontract agreement. For understandable reasons, prime contractors tend to manage internal risks within their own companies better than they manage risks that arise among suppliers. Proactive communication with and management of your suppliers, particularly key suppliers, is critical in avoiding surprises that may disrupt the program and reduce customer satisfaction.

Even scarier, a prime contractor's risk exposure to legal sanctions can extend to third parties in its supply chain, particularly if the exposure might lead to proceedings under the civil False Claims Act (FCA).[25] The FCA imposes liability on contractors for knowingly presenting to the Government, directly or indirectly, a false claim for payment.[26] Of particular concern in the supply chain context, the FCA can also impose liability on contractors if they knowingly *cause the submission* of a false claim for payment or make or *use* false records or statements material to a false claim.[27] Although the FCA requires that actions be taken "knowingly," that term is elastic and can include acts taken with "reckless disregard" or "deliberate ignorance" of the truth or falsity of the information.[28] Some courts have gone even farther and imposed liability under a theory of "implied certification," under which theory a claim for payment carries with it an unexpressed certification of compliance with material contract terms or regulations.[29]

While the subcontractor that submits false information to the prime contractor or higher tier subcontractor will be liable under the FCA in the first instance, the prime contractor may also find itself exposed by the subcontractor's conduct. 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 a subcontractor or based on false statements or certifications initially made by a subcontractor. You must therefore be alert for red flags or potential issues and consider taking steps necessary to ensure that any such reliance is reasonable. In addition, you may want to consider protecting yourself from the financial consequences of such reliance by requiring your suppliers to indemnify you against any FCA liability that might arise from the subcontractors' false claims or statements.

■ Vetting Subcontractors

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. Government contractors should use the "Excluded Parties List System," known as EPLS, to identify issues. This list can be accessed by contractors by signing up on the System for Award Management (SAM) website.[30] Contractors can also purchase information on suppliers through companies such as Dun & Bradstreet. There is 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 four key points:

(1) How to identify and confirm the qualifications of a potential supplier, including its business reputation and responsibility;

(2) How to confirm the business need and justification for working with the potential supplier;

(3) How to ensure that the necessary prime contract requirements and provisions are flowed down; and

(4) How to conduct ongoing monitoring of the supplier during subcontract performance.

When you are vetting potential suppliers, you may want to evaluate the suppliers' willingness to accept the necessary flowdown clauses required by the FAR, the supplier's ability and willingness to fulfill its duty to flow down such clauses to subtier suppliers, the supplier's willingness to fulfill its reporting obligations and otherwise cooperate with you, and the supplier's willingness to allow access to its own supply chain.

Subcontractor Source Selection, Responsibility & Past Performance

■ Source Selection

The Government uses extensive source selection resources to select prime contractors. Although the Government does not generally choose (or have "privity of contract"—i.e., a direct legal relationship—with) subcontractors and suppliers, the Government's source selection criteria may include an assessment of the prime contractor's ability to select and manage the suppliers it proposes to use to perform the contract.[31] Suppliers can play an important role in the competition for the award of prime contracts. They often provide key technical capabilities and may assist in developing a competitive cost volume or preparing the technical proposal. As noted later in the discussion of team arrangements, competition today is often between multinational teams of companies. In such cases, source selection officials will consider the management abilities of the prime contractor and the combined technical capabilities of the entire team—the prime contractor and its suppliers.

In seeking the competitive benefits provided by a strong team of subcontractors, however, prime contractors must avoid the potential for anticompetitive behavior. Subcontractors must be selected for legitimate purposes, 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 (and directed to report) unusual or restrictive bidding patterns that may suggest market sharing agreements or price collusion.[32] The FAR's subpart on contractor team arrangements expressly notes that "[n]othing in this subpart authorizes contractor team arrangements in violation of antitrust statutes."[33]

■ Responsibility

When selecting subcontractors, prime contractors should identify any flags that arise in connection with the subcontractor's "responsibility," such as repeated performance problems or ethical lapses. These issues can hinder the prime contractor's ability to win, and successfully perform, the contract.

The FAR states that "[p]urchases shall be made from, and contracts shall be awarded to, responsible prospective contractors only."[34] The standards for "responsibility" are found in FAR 9.104. The FAR makes clear that prime contractors should consider equivalent standards in evaluating and selecting subcontractors:[35]

> 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.

Also, while the FAR makes prime contractors responsible for determining the responsibility of proposed subcontractors, it 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.[36]

You should consider the FAR responsibility standards as a starting point for your own due diligence review of potential subcontractors. In addition, you may be well advised to include language in your subcontract agreements that allows termination if a later determination is made that the potential subcontractor lacks present responsibility. Where a teaming agreement is used, this contingency should be addressed in the agreement. Of course, such a determination is likely to negatively impact the prime contractor's chances for award—which reinforces the importance of due diligence in subcontractor selection.

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

(1) Have adequate financial resources to perform the contract (or subcontract) or the ability to obtain them;

(2) Be able to comply with the required or proposed delivery or performance schedule, taking into consideration all existing commercial and governmental business commitments;

(3) Have a satisfactory performance record;

(4) Have a satisfactory record of integrity and business ethics;

(5) 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);

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

(7) Be otherwise qualified and eligible to receive an award under applicable laws and regulations.[37]

Finally, contractors must 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" and, other than in a purchase of commercially available off-the-shelf (COTS) items, may not enter "into any subcontract, in excess of $35,000" with an entity "that is debarred, suspended, or proposed for debarment by any executive agency unless there is a compelling reason to do so."[38] Where the prime contractor believes it important and desirable to enter into a subcontract with a debarred or suspended party, the prime contractor must provide advance written notice to the CO.[39] To address these restrictions, prime contractors and higher-tier subcontractors should implement internal controls for confirming and documenting the status of prospective subcontractors and, if necessary, providing written notice to the CO.

■ Past Performance

The FAR makes past performance a factor in almost all source selections[40] and includes detailed provisions for collecting and maintaining contractor performance information.[41] Past performance information related to proposed subcontractors, particularly key subcontractors, can be an important part of an offeror's overall past performance rating and be a competitive discriminator.

Since 2010, the FAR has required the use of the Federal Awardee Performance and Integrity Information System (FAPIIS). FAPIIS consolidates information from the 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 nonresponsibility 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. 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.[42]

The purpose of this database is to enable COs to monitor the integrity and past performance of companies performing federal contracts, grants, and cooperative agreements. Indeed, the FAR requires 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.[43]

The Excluded Parties list is publicly available, which makes it easy for prime contractors to determine whether a potential subcontractor has been suspended or debarred. There are also automated subcontractor screening systems available to prime contractors, which can compare a company's subcontractor base and new subcontractors against the EPL and provide mechanisms in the company's purchasing systems that block purchases from any debarred or suspended subcontractor. The publicly available portions of SAM and FAPIIS do not, however, include past performance information compiled (in PPIRS and CPARS). Therefore, prime contractors can obtain this information only from proposed subcontractors themselves. Additionally, because all claims against subcontractors do not mature into litigation and are typically compromised with little attention, it is important for contractors to inquire within its organization regarding the past performance of its subcontractors. Before it relies on a potential subcontractor's past performance record, a prime contractor is well advised to review the subcontractor's past performance history, particularly if it is a new subcontractor with which the prime contractor has not previously conducted business.

■ Other Subcontractor Source Selection Considerations

Prime contractors must comply with "Competition in Subcontracting" requirements if the FAR clause is included in the contract and select subcontractors on a competitive basis, to the maximum practical extent, consistent with the objectives and requirements of the contract.[44] 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. However, statements by a prime contractor to justify a noncompetitive 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. Accordingly, you should consider creating templates to record—and preserve—justification and internal approvals for single-source, sole- source, and customer- or contractor-directed procurements.

Teaming & Collaborative Arrangements

Teaming and other collaborative arrangements, such as joint ventures, are common in Government contracting. Such arrangements can offer a working arrangement that extends through both the pursuit and performance of a Government contract. A teaming relationship involves collaboration prior to contract award, not just a purchase order or a subcontract issued only after the prime contractor has been selected for contract award. Indeed, the past performance, experience, and personnel of the teaming partner may be an essential part of the proposal to satisfy the requirements of the request for proposals (RFP). Teaming arrangements are popular because these arrangements can effectively pool the strengths of companies and combine complementary skills, spread risks, and assist in developing competitive strategies to address fierce competition for contract awards.

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.

Some may mistakenly believe that the process of forming a team—a team that may at times include competitors—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.[45]

■ Deciding To Team

When you are deciding whether to team, the first question to ask is whether a postaward 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 postaward subcontract. Important subcontractors may be willing to provide bid and proposal information and support only if the prime contractor will make a commitment to award a subcontract, something that a teaming agreement can provide. An opportunity may require the combination of specific complementary capabilities that are beyond the capabilities of single prime contractor. To be responsive to customer requirements, such as are found in major system RFP's, it is common for companies to team so that they can offer the full range of required capabilities.

The FAR 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. Team arrangements must be identified and disclosed, however, and the Government will maintain the right to hold the prime contractor fully responsible for contract performance.[46]

■ Benefits Of A Team Arrangement

The most important benefit of a team arrangement 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.

The legal obligations in a team arrangement may, however, limit certain options. For example, the team arrangement may assure a source for certain work, which may inhibit a change in the prime contractor's desire to "make" rather than "buy." Teaming with a company possessing the same core competencies may flag an examination of anticompetitive issues. The FAR specifically forbids team arrangements that are "in violation of antitrust statutes."[47] In particular, the FAR specifically cites, 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."[48] Teaming agreements between competitors may appear to be collusive when they include multiple contracting opportunities or will extend past the target procurement. A team arrangement can be challenged on antitrust grounds even if the agency had advance knowledge that the contractors intended to form a team arrangement, and even if the agency encouraged the arrangement.

For a team 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 negotiation leverage may change at contract award. A team member that is vital to winning the award but replaceable thereafter may be left 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 upon award—or at least that may be the prime contractor's fear.

Different approaches are possible when considering workshare allocation. If the contractual scope of work is well defined, it may be possible to allocate teammate responsibility by subject area. This may be difficult, however, in situations where the statement of work is evolving or for "umbrella" contracts with generic statement of work that become specific only in task orders. Some teaming agreements and subcontracts attempt to promise a workshare of a target percentage, or dollar amount, but this can be problematic. Other agreements include "eat what you kill" provisions, which are more common for task or delivery orders under an umbrella contract and reward the teaming partner for its marketing efforts.

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

■ Due Diligence Is A Necessary Step

Prime contractors should conduct appropriate due diligence before agreeing to team with a potential subcontractor. This is true even for a simple arm's-length purchase order negotiation, and it is far more important when the parties will be working closely together to pursue a contract—especially if they have not previously worked together. 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 that imposes legal obligations. Even if a due diligence inquiry does not reveal "show-stopping" red flags, it should provide important insight into the potential subcontractor as well as into terms and conditions that will be needed in the teaming agreement and subsequent subcontract to protect the prime contractor's interests. The teaming agreement must go beyond a form with standard boilerplate clauses; it should include tailored provisions resulting from the due diligence inquiry. Areas requiring such tailoring typically include ownership of joint intellectual property, exclusivity, proposed work allocations, and prime contract flowdowns.

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.

Organizational conflict-of-interest (OCI) issues[49] and personal conflict-of-interest (PCI)[50] issues should also be considered and evaluated. For example, an OCI may arise if a teaming partner has had access to nonpublic information related to the procurement, had input into the statement of work or specification or performed Systems

Engineering and Technical Assistance (SETA) in the program, or has business interests that could be affected by performance of the contract.[51] The inclusion of a team member with an OCI problem or a team member with employees who may pose PCI problems could lead to a disqualification of the team unless the OCI or PCI can be mitigated.[52]

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

■ Exclusivity

A question that teammates must consider is whether the arrangement should be exclusive—i.e., whether teammates will be allowed to join different teams in competition for the same contract award. When companies collaborate to prepare a proposal in response to an RFP, they typically share proprietary information, including pricing and strategies. An arrangement that is not exclusive tends to inhibit the free flow of information out of concern that this information will leak. When a teaming partner plays on multiple teams, it often must 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 where small businesses with limited staffs are involved.

The agencies charged with policing anticompetitive behaviors, including the Federal Trade Commission and the U.S. Department of Justice, 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.[53] That said, exclusive arrangements do raise questions of possible anticompetitive impact, which should be analyzed prior to formalizing a teaming relationship.

■ Enforceability

An issue that accompanies the formation of a teaming agreement is whether the agreement is an enforceable agreement or merely an unenforceable "agreement to agree." Although the vast majority of disputes between team members are resolved through negotiation or the use of alternative dispute resolution mechanisms such as mediation or arbitration, some disputes do proceed into the court system. A number of judicial decisions have addressed whether the court should enforce a particular teaming agreement. Decisions are mixed, but in general a teaming agreement will be enforceable in court only if there is a clear intent to be bound, adequate consideration, and sufficient agreement on material terms of the subcontract.

These factors can be difficult to define if the program's requirements are not finalized at the time the parties negotiate the teaming agreement. The reality is that under the time pressures of competition it is often not possible to negotiate a definite subcontract that will be legally enforceable. Moreover, there may be times when one or the other party prefers that the teaming arrangement not be enforceable. 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.

■ Flowdowns

Subcontracts and teaming agreements will generally contain "flowdown" requirements that mirror (and often copy) provisions in the prime contract. Many "mandatory flowdown" clauses are required by the FAR or the prime contract clause. Other clauses are discretionary flowdowns; they are not required by the contract or regulation but may be necessary as a business matter to protect the prime contractor's interests. For example, if appropriate versions of the "Changes" clause and the "Termination for Convenience of the Government" clause are not "flowed down" to the subcontractor, the prime may find itself caught between a unilateral change order or termination from the Government and a subcontractor that refuses to perform the changed work or claims breach of contract.

While the flowdown clauses will be based on the prime contract, they should be tailored as appropriate. Due to their volume of solicitations, most large prime contractors will reference in their teaming agreements certain subcontract templates that are to be negotiated with the subcontractor in the event that the contractor is awarded a prime contract. Such subcontract templates contain FAR and DFARS clauses that will likely apply to the subcontractor. As an example, Raytheon's "Solicitation Attachment" is posted on its external "supplier resources" web page and labeled "TC-HARDCODE."[54] The requirements set forth in the TC-HARDCODE Solicitation Attachment are in addition to and not in place of the prospective supplier's requirements that are identified elsewhere in the RFP. As the requirements of a given acquisition become more defined, prime contractors will identify and flow down special provisions from the prime contract that will supplement the prime contractor's previously identified clauses. Accordingly, it is important for potential subcontractors to ensure that they have received and can satisfy the requirements of all required flowdown clauses.

Where there is more than one level of subcontractor, flowdown requirements can extend to lower tier subcontractors. A subcontractor's failure—at any level—to satisfy the requirements of a mandatory flowdown provision can force a prime contractor into a situation where the customer may successfully terminate the prime contract for default, exposing the prime contractor to damages.

Policies, Procedures & Standard Forms & Agreements

Government contractors understand the benefits of developing and communicating policies and procedures that address the contractor's operating principles, strategy, and goals. Such policies may be consistent with statutory, regulatory, customer, and management requirements. They should be consistent across the organization and, ideally, they should institutionalize best practices.

■ Developing Supply Chain Policies & Procedures

The supply chain function is a key function for the development of company policies and procedures to ensure compliance with the contractor's operating principles, because the function addresses a broad range of statutory, regulatory, and customer requirements and reaches the many third parties essential for the successful performance of the contractor's contracts. In light of this broad scope, the supply chain function will typically work collaboratively with other contractor functions to develop and implement policies and procedures that are most efficient and effective for the contractor's governance. For example, Raytheon's Integrated Contracts and Supply Chain function leads the Acquisition Policy Council in soliciting internal cross-functional comments regarding proposed regulations and defense industry group communications with Government customers. The Acquisition Policy Council briefs all Raytheon business units on developing legal and regulatory requirements and works with applicable company functions in developing and implementing policies and procedures to ensure compliance.

Functional coordination goes even further. In coordination with Raytheon's Acquisition Policy Council, Raytheon's Subcontract Advisory Group, a cross-functional/cross-business Group led by Raytheon's Legal function, prepares enterprise-wide guidance with respect to select subcontract management and compliance topics; creates procurement and subcontracting processes and model contract terms and conditions for enterprise-wide use; and ensures that standard subcontract and procurement document templates remain current.

According to a 2015 Government Accountability Office report, between 2010 and 2014 the DOD published 279 final and interim DFARS rules.[55] Each became effective immediately, yet approximately half were issued without prior notice and comment.[56] The frequency of unannounced changes requires defense contractors to coordinate their internal cross-functional and business teams and to benchmark with others in the defense industry to keep current regarding their supply chain compliance needs.

For Government contractors, supply chain policies are vital to successful performance and compliance and play an important role in the business system approval process. When the DCMA conducts an onsite CPSR, it attempts to assess the overall health of the contractor's purchasing organization and the efficiency and effectiveness of the contractor's practices. Much of the CPSR is based on an examination of the contractor's purchasing policies, procedures, and practices.

Due to the high level of outsourcing of certain functional responsibilities, contractors must frequently incorporate applicable company policies and procedures into provider agreements and flow them down, along with applicable FAR and DFARS clauses. To facilitate this process—and particularly to provide guidance to commercial item suppliers that may not have sophisticated Government contracting experience—many contractors will post legal, regulatory, and business information on their public websites. Indeed, it has become common for companies to include a supplier "resource" link on their public websites, which may include policies, procedures, and standard supply chain contract terms. Making these documents available on its website can provide transparency to the sourcing process and expedite the teaming and subcontracting process.

■ Standard Supply Chain Terms & Conditions & Related Certification & Compliance Documents

A company's supply chain function can benefit from the development and use of standard supply chain terms and conditions templates and standard certification and compliance documents. A company may develop several different standard forms to address various types of purchasing situations.

Depending on the nature of the contractor's products, services, contracts, and supply chain requirements, and whether it typically acts as prime contractor, subcontractor, or (at different times) both, a contractor might have separate forms to cover (a) general purchasing (applicable to both Government and commercial programs), (b) Government-specific terms and conditions (applicable to purchasing under Government programs), (c) agency-specific terms and conditions (applicable to purchasing for particular agency programs, such as the DOD), (d) commercial item terms and conditions (applicable to "commercial item" subcontracting), (e) international terms and conditions, and (f) updated regulatory requirements (useful to highlight changes in the basic subcontracting forms and, in some cases, to reduce the need to make frequent revisions). A contractor might also have standard forms for frequently used agreements, such as nondisclosure agreements, teaming agreements, and long-term agreements that are entered into between contractors and subcontractors to establish pricing for future purchases of specified items.

For example, on its "Supplier Resources" website Raytheon provides links to its General Terms and Conditions of Purchase and explains that they are incorporated by reference on Raytheon purchase orders.[57] The General Terms and Conditions include several standard forms that address the types of supplier agreements encountered on a regular basis. In some cases, these standard templates include embedded links to various other forms for subcontractors to reference and use. Raytheon's International Terms and Conditions of Purchase (TC-004) includes embedded links to the "Consolidated Screening" or "Restricted Party" List, which is a list of parties for which the U.S. Government maintains restrictions on certain exports, reexports, or transfers of items. There is a link to an "International Traffic in Arms Regulations Certificate and Reporting of Political Contributions, Fees or Commissions" (IN-009) template for complying with reporting requirements under Part 130 of the International Traffic in Arms Regulations (ITAR).[58] There is also a link to Raytheon's Code of Conduct. The website also includes archived versions of the most heavily used standard terms and conditions templates. Raytheon's TC-HARDCODE template,[59] referenced earlier in this Paper, contains several links to additional terms and conditions and relevant documents, including a link to Raytheon's Supplier Jurisdiction and Classification Certification template, which requires an applicable supplier to provide Raytheon with the export classification of any deliverable that is subject to the ITAR[60] or the Export Administration Regulations (EAR)[61] in advance of providing such a deliverable to Raytheon. The "TC-Update" document immediately updates lists of FAR and DFARS flowdown clauses and incorporates the new clauses into agreements by reference, and Raytheon's Software License Agreement Addendum (IP-006) is designed to amend subcontractor software license agreement templates to include appropriate software use rights and other required provisions when the end user of the software is the U.S. Government.

Raytheon also posts several standard certification templates on its external Supplier Resources web page.[62] For example, the "Annual Offeror Registration Data, Representations and Certifications (CR-003)" document collects certain business data and particular representations and certifications that are required to provide goods or services in support of a U.S. Government contract. In addition, the "Assertion of Commerciality Certification (CR-006)" document is designed to obtain and record a subcontractor's assertion of commerciality for its goods, software, or services ("item"). Raytheon can use the subcontractor's CR-006 response, along with information from public sources, commercial price sheets and catalog information, and product specification sheets, to substantiate and document that the item meets the definition of "commercial item."

Supplier Business Ethics & Conduct

All contractors today understand the need for business ethics and conduct. Indeed, the defense industry was an early adopter of codes of ethical conduct, starting with the voluntary Defense Industry Initiative (DII).[63] The DII was started in 1986, when the defense industry was suffering through a spare parts pricing scandal that provided fodder to late night talk show host monologues and resulted in general mistrust of the industry. Over time, the principles of the DII, along with similar principles found in the United States Sentencing Commission *Guidelines Manual*,[64] have been adopted by most defense contractors and woven into the fabric of the FAR. What began as a voluntary commitment with the DII has evolved into a FAR mandate—that extends to the supply chain.

■ Business Ethics & Conduct

The FAR is clear on what is required. Contracts with a value expected to exceed $5.5 million (and with a performance period of 120 days or more) contain the "Contractor Code of Business Ethics and Conduct" clause.[65] 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 its Government contracts and subcontracts (specifically, violations of federal criminal law involving fraud, conflict of interest, bribery or gratuities, or violations of the civil FCA).[66] Additional FAR commitments apply unless the contract is for commercial items or with a small business; these 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 and to report possible violations of the Anti-Kickback Act[67] when the contractor "has reasonable grounds to believe that [such a] violation may have occurred."[68] 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 for the purposes of "improperly obtaining or rewarding favorable treatment" in connection with a prime contract or subcontract.[69]

■ Flowing Ethics Down Into The Supply Chain

The "Contractor Code of Business Ethics and Conduct" clause extends to subcontractors in several 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 or another subcontractor").[70]

(2) The business ethics awareness and compliance program commitment includes

training for agents and subcontractors "as appropriate."[71]

(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.[72]

(4) 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."[73]

As part of the supplier selection process, prime contractors should consider the business ethics program of potential suppliers, especially those with whom the prime has no prior working relationship. That is the time when a prime contractor may have the most leverage to obtain this information, because the supplier may be in competition with other potential suppliers to join the team. In addition, prime contractors may have—or may want to develop—standard terms that require notifications and ongoing access to information concerning ethics and compliance issues.

During performance, prime contractors should monitor suppliers, not only for their technical and cost results, but also for issues relating to their 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 not defined and can be subjective; and (b) relationships between a prime contractor and its suppliers often encompass not only Government business (where kickbacks are illegal) but also commercial business (where gratuities may be permissible).

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 supplier'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 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. In addition, a prime contractor might face litigation exposure if a subcontractor believes that the prime's communications to the Government contains derogatory misinformation about the subcontractor.

Counterfeit Parts

Counterfeit parts in the supply chain represent a significant threat to end users and are a major concern of Government buyers. As noted in a recent Briefing Paper on this subject, the last several years have witnessed "an epidemic of counterfeit items—electronic components, in particular—in the supply chains of defense contractors."[74]

Responding to the concern that a flood of counterfeit electronic parts were entering the defense supply chain and endangering our troops, Congress mandated that the Secretary of Defense assess the DOD's "acquisition policies and systems for the detection and avoidance of counterfeit electronic parts" and disallow certain costs associated with counterfeit electronic parts.[75] As mandated by this legislation, on May 6, 2014, the DOD issued a final DFARS rule requiring that contractors establish and maintain a risk-based electronic system to monitor, detect, and eliminate counterfeit parts.[76]

Concern over counterfeit parts, by its very nature, implicates the supply chain from which most parts are obtained. In fact, not only does the DFARS rule apply 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.[77] It even reaches commercial items and

COTS items if those items are being supplied to a CAS-covered contractor. This means that prime contractors and higher tier subcontractors must pay close attention to the commercial suppliers and vendors in their supply chains. Although the current rule is limited to the DOD, it provides a model for a detection and avoidance 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.

■ DFARS Counterfeit Electronic Parts Rule

The DFARS "Contractor Counterfeit Electronic Part Detection and Avoidance System" clause provides an outline for an adequate counterfeit part detection and avoidance system.[78] The contractor must comply with the DFARS rule if it is providing the DOD with electronic parts, end items, components, parts or assemblies containing electronic parts, and services where the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the services.[79] The DFARS rule applies to counterfeit electronic parts, suspect electronic parts, and obsolete electronic parts, including any embedded software or firmware. These terms are defined in the rule.[80]

■ Standards

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 12 attributes:[81]

(1) Training as appropriate, based upon the contractor's needs.

(2) Tests and inspections, "based on minimizing risk to the Government."

(3) Reporting 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) Traceability of the electronic part to the original manufacturer. The rule does not require any particular procedure, but requires 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 from original manufacturers or authorized sources, or from suppliers that "meet applicable counterfeit detection and avoidance system criteria."

(6) Retention of counterfeit or suspect counterfeit parts "until such time that the parts are determined to be authentic."

(7) Use of a risk-based methodology to "rapidly determine if a suspect counterfeit part is, in fact, counterfeit."

(8) Systems to detect and avoid counterfeit and suspect electronic parts, which may use "current Government- or industry-recognized standards."

(9) Flowdown of counterfeit detection and avoidance requirements to subcontractors and suppliers at all levels. This emphasizes the need to police the entire global supply chain, including commercial subcontractors.

(10) Processes to keep informed of counterfeiting issues and use current information and trends to continuously upgrade internal procedures.

(11) Review of GIDEP and other credible reports of counterfeit parts that could affect their supply chains.

(12) Control of obsolete electronic parts to maximize the availability and use of authentic parts during the products life cycle.

■ Government Review & Remedies

The Government reviews compliance with the DFARS counterfeit parts rule through the CPSR. The rule's preamble states that CPSRs will examine the contractor's policies and procedures for the detection and the avoidance of counterfeit electronic parts. If the DCMA identifies a "significant deficiency"—i.e., a shortcoming in the system that materially affects the ability of the DOD to rely upon the purchasing system—the CO can decide to disapprove the contractor's purchasing system and to withhold payment.[82]

The rule also has important cost recovery implications. A new section of the DFARS cost principles 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 (a) the contractor's system for detecting and avoiding counterfeit electronic parts has been reviewed and approved by the Government, (b) the parts were Government-furnished, *and* (c) the contractor provides notice within 60 days of becoming aware of the counterfeit or suspect counterfeit electronic part.[83]

The bottom line: noncompliance with the counterfeit parts rule threatens the contractor's ability to conduct business with the Government.

■ Anticipated Broader Rule

The current DFARS rule represents the type of system that the Government expects to see and provides a model for contractors. Although the current rule is limited to the DOD, a broader Government-wide rule is anticipated. The Federal Acquisition Regulatory Council has issued a proposed rule that would require anti-counterfeiting systems in civilian agencies and include nonelectronic parts.[84]

Cybersecurity

Cybersecurity concerns are among the Government's top issues, and Government contractors are subject to an increasing array of rules and responsibilities. Many of those rules and restrictions address the supply chains because each level of chain is a potential point of cyber risk for the Government customer and a back door prime contractor or Government information. The regulatory environment regarding cybersecurity is in a state of rapid evolution and is most advanced in the DOD. Accordingly, this is a snapshot of several of the major DOD requirements that exist as of Fall 2015.

■ DFARS Supply Chain Risk Rule

In November 2013, the DOD published an interim rule[85] amending the DFARS to address supply chain cyber risk. The rule put in place a DFARS pilot program to implement statutory direction to address the impact of information technology supply chain risk in certain types of procurements related to national security systems.[86]

Almost two years later, on October 30, 2015, the DOD adopted the interim rule, but with certain important changes.[87] The final rule allows the DOD to consider the impact of supply chain risk in specified types of procurements related to national security systems. This rule reflects congressional concern over supply chain risk in technology contracts supporting the DOD: "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[88]

New guidance covers the use of a competitive evaluation factor regarding supply chain risk. It mandates the evaluation factor when acquiring information technology, whether as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system. The final rule notes that suppliers are expected to manage supply chain risk, and provides that sources may be excluded during source selection process (through the evaluation factor) or after award (by withholding consent to a subcontract).[89] Significantly, there is no exemption for acquisitions below the simplified acquisition threshold (SAT) or for commercial items or COTS, because such an exemption would not be in the "best interest of the United States."[90]

■ Covered Defense Information & Network Penetration Reporting Rule

In August 2015, the DOD issued an interim rule amending the DFARS to implement sections of the National Defense Authorization Acts for Fiscal Years 2013 and 2015 that require contractor reporting on network penetrations.[91] The rule expands on and revises an earlier DFARS provision from 2013 that required contractors (a) to implement National Institute of Standards and Technology (NIST) standards for protection of information, and (b) to report a cyber incident involving unclassified controlled technical information to the DOD within 72 hours of the incident. The interim rule is broader and encompasses "covered defense information," which includes unclassified controlled technical information as well as export-controlled information, critical information (operations security), and any other information marked or otherwise identified in a defense contract that requires safeguarding or dissemination controls.[92] It also calls for implementation of a more targeted set of National Institute of Standards and Technology (NIST) standards contained in NIST Special Publication (SP) 800-171.[93]

The interim rule's implementing DFARS clauses contain flowdown requirements. Under the interim rule, subcontractors are obligated to report cyber incidents both to the prime contractor and to the DOD.[94] There is a separate DFARS clause to protect third-party information from disclosure by support contractors that deal with cyber reports.[95]

Contractors have expressed many compliance concerns through the comment process since the interim rule was issued. One consistently cited concern is over the contractor's and subcontractor's ability to comply with 109 new NIST requirements. In response to this challenge, many contractors and subcontractors are likely to submit requests to deviate from the security requirements in NIST SP 800-171, either by proposing alternative but equally effective security measures or by demonstrating why a particular requirement is not applicable. Such requests are contemplated under the DFARS "Compliance With Safeguarding Covered Defense Information Controls" clause[96] and require DOD Chief Information Officer (CIO) approval "prior to contract award."[97] The clause prescription seemingly requires contractors and subcontractors to request a deviation of this type every time a proposal is submitted.[98] Moreover, it is unclear from the clause if subcontractors may request such deviations directly or must request them through the prime contractor and what, if any, role the prime contractor plays in the process. These transaction-specific requirements could result in tremendous inefficiencies and transactional, compliance, and economic burdens on the supply chain.

■ Intelligence Community Directive

The Intelligence Community (IC) is also identifying supply chain cyber risks. The IC operates under its Directive called "Supply Chain Risk Management," which outlines the contractor's duties and responsibilities to protect its supply chain.[99] 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 Government. This IC Directive allows the exclusion of contractors, subcontractors, or vendors from procurements of information technology based on supply chain risk factors that are identified during a risk assessment. In addition, the disclosure of information relating to that exclusion may be limited to protect national security. This Directive is similar to the recently issued DFARS final rule on supply chain risk.[100]

■ China Sourcing Restrictions

The continuing resolution to fund federal agencies through the rest of fiscal year 2013 included a provision that addresses the concern of Congress over risks posed by technology imported from the People's Republic of China. This provision prohibits the Departments of Commerce and Justice, the National Aeronautics and Space Administration, and the National Science Foundation from purchasing information technology 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 Federal Bureau of Investigation and a determination is made that the purchase is "in the national interest of the United States."[101]

Intellectual Property

The regulatory regime for allocating rights in intellectual property (called "data rights") between the Government and prime contractors can implicate the entire supply chain.

■ Technical Data & 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 defined in both the FAR, which applies to civilian Government agencies, and the DFARS, which applies to DOD agencies. It should be noted that this is one of the rare instances in which the DFARS supplants, rather than supplements, the FAR. It is useful to use the DFARS as the baseline for understanding the rules, because the DOD tends to be ahead of the curve in its contracting practices, which is not surprising because it engages in many more contracting actions involving "data rights."

Under the DFARS, rights in noncommercial technical data and computer software are generally allocated through different categories of license rights granted by the contractor to the Government. The Government's license rights will generally depend on the source of funding. The Government generally gets "unlimited rights" in data and software when they are funded exclusively at public expense, "limited" or (per the FAR) "restricted" rights when they are funded exclusively at private expense, or "Government purpose license (GPL) rights" when they results from mixed funding.[102] With limited exceptions the Government does not obtain ownership of the data or software; rather, the contractor usually retains ownership, as well as all rights that are not granted to the Government by the contractual license,[103] and is free to use it or license it to other customers.

Protection of rights in technical data and computer software is subject to a number of procedural hurdles. 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).[104] The FAR permits inclusion of a similar clause.[105]

When a contractor delivers to the Government technical data and computer software with less than unlimited rights, the contractor must mark the data or software with a prescribed restrictive legend, set forth in the FAR and DFARS, describing the rights that the Government is obtaining.[106] These pre-notification and marking requirements are important; failure to comply may waive contractor's rights, resulting in the Government obtaining greater rights than were intended or justified.[107] This makes it vital for DOD contractors (and their subcontractors) to have written procedures for ensuring appropriate use of restrictive legends and to maintain documentation sufficient to justify any claimed restrictions on the Government's right to use or disclose data or software.[108]

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.[109] Deferred ordering or delivery also extends to subcontractor data or software.

Consistent with Government procurement policy, purchase of commercial software or data is less encumbered by Government rights and restrictions. For "commercial items," the DFARS specifies that DOD agencies are to obtain only technical data that are 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.[110] 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 the terms of 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.[111] Technical data related to commercial items must still be properly marked, however, or else the Government can assert an unrestricted right to use or disclose the data.[112]

The FAR coverage for technical data for commercial items and commercial computer software is similar. The FAR 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."[113] 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 the FAR.[114] The FAR also permits use of a "Commercial Computer Software License" clause, although its terms are not consistent with many commercial license terms.[115]

■ Technical Data & Computer Software & Subcontracts

The DFARS expressly requires that certain contract clauses pertaining to technical data and computer software be flowed down to subcontractors. These mandatory flowdown clauses include the basic rights in noncommercial data and computer software clauses and clauses that relate to the Government's right to challenge restrictive markings.[116] Other important clauses—for example, those relating to deferred delivery or deferred ordering—are not specifically required to be flowed down, 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.

Even though prime contractors should not normally require ownership rights in their subcontractors' noncommercial data or software, they may still need to obtain license agreements if they need to use subcontractor data or software to perform the prime contract. Sometimes, however, a prime contractor may seek data rights that go beyond what is necessary for successful contract performance. As a result, ownership of and license to data and computer software can become a bone of contention between prime contractor and subcontractor, especially if they are competitors in other programs. The DFARS has specific language that can protect subcontractors in this battle. Specifically, the DFARS has contract clauses that 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 to subcontractor data.[117]

The DFARS also prohibits the Government 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 contract or subcontract.[118]

As noted earlier, both prime contractor and subcontractor technical data and computer software should be properly marked to limit the Government's rights, and the DFARS places an obligation on prime contractors to ensure that subcontractor rights are adequately protected in the identification, assertion, and delivery processes.[119] Although communications with the Government relating to contract administration are generally made by and through the prime contractor, the DFARS permits the Government to communicate directly with the subcontractors (without creating privity of contract) with respect to validation of or challenges to restrictive markings on subcontractor technical data or computer software.[120] Subcontractors also can submit technical data with other than unlimited rights directly to the Government, rather than through the prime contractor.[121]

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.[122] If a subcontractor refuses to accept terms granting the Government those rights, the FAR clause directs the prime contractor to notify the CO and prohibits the prime contractor from proceeding with award of the subcontract without authorization from the CO.[123]

Prime contractors holding contracts that include the DFARS clause "Technical Data—Commercial Items" must include that clause in subcontracts under their prime contracts where technical data will be obtained from the subcontractor for delivery to the Government.[124] There is no similar mandatory flow down requirement for the FAR clause "Commercial Computer Software—Restricted Rights."[125] 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).

■ Patent Rights

Under the standard FAR and DFARS "Patent Rights" clauses, 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."[126] 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 "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.[127]

The standard "Patent Rights" clauses include numerous procedural provisions, requiring the contractor to disclose subject inventions to the CO; elect to retain title to subject inventions, and file patent applications in subject inventions in which the contractor has elected to retain rights.[128] As is the case with software and data, failure to follow these procedural steps within the prescribed times can result in loss of rights by the contractor.

■ Patent Rights & Subcontracts

The DFARS "Patent Rights" clause 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.[129] The FAR "Patent Rights" clause is essentially the same in this regard. [130]

■ Authorization & 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.[131] Instead, an aggrieved patent or copyright holder is limited to a suit against the United States for royalties.

This protection 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. The FAR "Authorization and Consent" clause provides this protection from injunctive relief to any invention covered by a patent that is "[e]mbodied in the structure or composition of any article…accepted by the Government," or "[u]sed in machinery, tools, or methods" resulting from compliance by the contractor or subcontractor with contract specifications or provisions or written instructions from the CO.[132] An alternative version, 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."[133] 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.[134]

These protections can be very important to prime contractors and subcontractors. Most important, if a contractor is acting with the Government's "authorization and consent," it is unlikely that contract performance will be stymied by a badly timed injunction from an unfriendly court. In addition, the contractor (and subcontractor) will not have to incur the costs of litigating a patent or copyright infringement claim. This latter protection is not total, however, because the contractor (or possibly the subcontractor) may ultimately be required to indemnify the Government against patent royalty claims if the contract includes the FAR provision on patent indemnity.[135] This risk is usually low, however; royalty actions against the United States are infrequent because they are usually very time-consuming and expensive to bring.

■ Other Potential Intellectual Property Issues

Many other intellectual property issues can arise in the supply chain context, but are outside the scope of this Briefing Paper. 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.[136]

Supply Chains & Socioeconomic Considerations

The procurement system can serve as a tool to implement and promote a number of public policies, including support for small businesses. These policies provide significant benefits to those supported, but they bring with them significant compliance risks as well.

■ Misrepresenting Small Business Size

When size status is relevant to award or performance of a contract, prime contractors and, where applicable, higher tier subcontractors, should verify and if needed monitor the size status of their small business subcontractors before and during contract performance. Misrepresenting a subcontractor's small business size status can result in severe penalties for both the prime contractor and subcontractors. When it is established that a contractor or subcontractor has misrepresented its size status as a small business and willfully sought and received an award for a contract, subcontract, or grant that was set aside, reserved, or otherwise classified as intended for award to a small business, Congress has implemented a presumption of loss to the Government equal to the total amount the Government expended on the contract.[137]

A broad range of actions can be deemed willful and give rise to potential criminal or civil liability. These actions include submitting a bid, proposal, application, or offer for a federal contract or grant (including cooperative agreements) that is reserved or set aside for a small business concern or that encourages a federal agency to classify the award as one to a small business concern.[138] A contractor may also be deemed to have willfully certified itself as a small business if it registers on any federal electronic database for the purpose of being considered as a small business for a federal grant or contract award.[139]

A finding of willful misrepresentation of small business status can result in severe consequences for those involved, including potential suspension, debarment, criminal prosecution under the Small Business Act,[140] civil or criminal remedies under the FCA,[141] and civil remedies under the Program Fraud Civil Remedies Act.[142] Under the civil FCA, for example, a false certification of small business status may result in contractor liability equal to treble damages of the presumed loss, which could be as much as three times the total amount the Government expended on the contract.[143]

Although the primary sanction for misrepresentation of a subcontractor's size status will fall on the subcontractor, a prime contractor could also be subject to civil or criminal penalties. If the prime contractor has exercised "due diligence," however, it should not be penalized for its good faith acceptance of representations made by its subcontractor. (For example, Raytheon uses its CR-003 Certification template, referenced earlier, to secure the subcontractor's certification as to its size status.) In assessing possible prime contractor liability, the Government generally considers (1) the contractor's internal management procedures governing size representations and certifications, (2) the clarity or ambiguity of the representation or certification requirements, and (3) the efforts made by the contractor to correct an incorrect or invalid certification or representation in a timely manner.

Thus, where size status is relevant to award eligibility or evaluation, it is important for small businesses to monitor their size eligibility and for large businesses seeking to subcontract with a small business to confirm and document the small business's representation of its size status. In particular, both large and small business should implement practices to make sure that agreements comply with any "performance of work" requirements (e.g., those that require a small business to perform a certain portion of the work) and do not cause the small business to lose its eligibility—i.e., that it does not become the victim of its own success.

■ Small Business Subcontracting Plans

The FAR requires large contractors to prepare and to comply with subcontracting plans for federal contracts or subcontracts for goods and services exceeding $700,000 (or $1.5 million for construction contracts).[144] (This requirement is not applicable for personal services contracts, contracts performed entirely outside the United States, or where the prime contractor is a small business.)[145] The subcontracting plans set forth how a contractor will provide to small business contractors the maximum practicable opportunity to participate in the performance of a federal contract or subcontracts. Large contractors must make good faith efforts to achieve the written goals established in their subcontracting plans.[146]

There are three types of subcontracting plans: (1) commercial plans, (2) individual plans, and (3) master plans. Commercial subcontracting plans are company-wide plans and are appropriate for contractors that furnish commercial products or services to both the Government and commercial customers. They are submitted annually and set forth the contractor's status, achievements, and compliance with its goals.[147]

An individual subcontracting plan applies to a specific contract and covers the entire contract period, including option periods. Individual plans will state separate dollar and percentage goals for the particular contract and must be negotiated and approved by the CO prior to award.[148] Contractors are generally required to submit annual subcontracting reports that set forth their status, achievements, and compliance with individual plan goals.[149]

Master subcontracting plans contain all of the required elements of an individual plan, without specific goals. Master plans are then supplemented by individual contract targets when contracts are awarded.[150] Master plans are in effect for three years, but may apply for the life of a particular contract if the plan is incorporated into an individual contract plan.[151]

Each subcontracting plan should contain the following elements:

(1) Separate percentage goals for using small businesses and other socioeconomic business categories (such as veteran-owned, women-owned, etc.);

(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 to each group;

(4) A description of the method used to develop the subcontracting goals;

(5) A description of the method used to identify potential sources;

(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;

(7) The name and duties of the administrator of the subcontracting plan;

(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 flow down the FAR small business clauses as required;

(10) Assurances that the contractor will cooperate in any studies or surveys and will submit periodic reports to the Government as required; and

(11) A description of the types of records that the contractor will maintain to demonstrate its compliance with its subcontracting plan.[152]

Contractors are not generally held strictly liable for missing a target, as long as they have made good faith efforts to reach that target and have followed their subcontracting plans in doing so. When that happens, however, a contractor should explain in writing why it did not meet its targets or follow the provisions of its plan. If a contractor fails to make a good faith effort, the Government may claim that it has materially breached its contract and the contractor may be subject to termination for default and/or liquidated damages equal to the actual dollar amount by which the contractor failed to achieve its subcontracting goals.[153]

A contractor's failure to meet its subcontracting goals can also cause harm to the contractor's future competitive position. Agencies are authorized to use subcontracting plan compliance as an evaluation factor in source selection.[154] Thus a contractor's ability to meet its subcontracting plans goals may factor into past performance evaluations.

Global Supply Chain Issues

Government contractors are increasingly engaged in opportunities abroad, for both the U.S. and foreign governments, and often rely on the global supply chain for domestic programs. The global span of supply chains brings into the compliance mix many laws that apply to global transactions, as well as the laws of other countries. (Consideration of non-U.S. laws is outside the scope of this Briefing Paper.) Many of these compliance issues were covered in depth in a previous Briefing Paper, *Managing International Regulatory Risk in the Government Contract Supply Chain.*[155]

■ Country-Of-Origin Restrictions

Several statutes and regulations impose country-of-origin restrictions on products sold to the U.S. Government. The most important are the Buy American Act (BAA)[156] and the Trade Agreements Acts (TAA).[157] These restrictions can have significant supply chain implications.

(1) *Buy American Act (BAA)*. The BAA 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 that fall under the Trade Agreements Act (TAA), discussed below, and in practice most acquisitions of supplies are 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 the United States must exceed 50% of the cost of all components.[158] The FAR defines a "component" in relevant part as "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.[159] The FAR does not define "manufactured"; however, case law can provide guidance. The "domestic end product" test is relaxed for COTS items; in those cases, the item must be "manufactured" in the United States but does not need to meet the 50% U.S. cost of components test.[160]

Several exceptions to the BAA permit the Government to acquire a "foreign end product." These include the "nonavailability" and "unreasonable price" of a domestic end product.[161] The BAA also does not apply to the acquisition of "information technology" that is a commercial item.[162] Finally, the DFARS allows the DOD more flexibility through the concepts of "qualifying country end product" and "qualifying country end component."[163]

(2) *Trade Agreements Act (TAA)*. The TAA and related FAR provisions[164] generally restrict the Government's purchase of products (and services) to "U.S.-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 nondiscriminatory treatment for public procurement purposes, and certain developing and Caribbean Basin countries. Countries such as China and India are currently not "designated countries."[165] The TAA applies to most acquisitions of supplies and services with an estimated value above a threshold that is adjusted every two years according to a predetermined formula. The current threshold is $204,000 ($7,864,000 for construction contracts), although some trade agreements have different dollar thresholds and some procurements are exempt from the TAA.[166]

The FAR 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 Subparts 6.2 or 6.3, and certain national defense related procurements.[167] The TAA also provides for "nonavailability" determinations.[168] However, the TAA does apply to contracts for commercial items, including General Services Administration Multiple Award Schedule contracts, and, unlike the BAA, does not include an exception for commercial information technology. Finally, the DFARS TAA clause permits acquisitions from "qualifying" as well as from "designated" countries.[169]

It is important—and sometimes confusing—to understand that the TAA definition of "U.S.-made" is different from the BAA definition of "domestic end product." Under the TAA, a "U.S.-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."[170] "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.[171]

Determining "substantial transformation" for TAA purposes is complex and considers the "totality of the circumstances," including:[172]

> 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.

■ Supply Chain Compliance Considerations

Country-of-origin requirements, such as the BAA and TAA, can have significant supply chain implications. Procurements subject to the BAA require careful analysis of the bill of material of the end product to ensure that the components meet U.S. 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. Recent case law indicates that a contractor can rely on a supplier's representation regarding country of origin, provided that the reliance is reasonable.[173]

Throughout this process, 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. Prime contractors might consider requiring 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. Where the TAA applies, the FAR requires the offeror to certify that the end products to be delivered are either U.S.-made or designated country end products, and to identify any that are not.[174] The FAR includes a similar certification regarding BAA compliance.[175] Therefore, country-of-origin requirements in the TAA and BAA should be approached with care and should be addressed prior to proposal submission and contract award.

BAA and TAA noncompliance can present significant issues for contractors. Bid protests challenging TAA compliance are becoming more frequent and have upended some contract awards. Courts and boards have upheld terminations for default based on BAA and TAA noncompliance. Noncompliance with country-of-origin requirements, including improper certifications of compliance, can result in Government or qui tam actions under the civil FCA, and there have been a number of multi-million dollar FCA settlements 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.[176]

■ Other Country-Of-Origin Restrictions

The BAA and TAA are not the only country-of-origin rules that apply to Government procurements. For example, the Berry Amendment, implemented in the DFARS,[177] essentially requires the DOD to buy certain textile and specialty metal products that are 100% domestic in origin, though there are certain complicated exceptions to this basic requirement. The American Recovery and Reinvestment Act of 2009 (ARRA), more commonly referred to as the Stimulus or the Recovery Act,[178] 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, the U.S. Agency for International Development (USAID) has special rules, entitled "Source and Nationality," that can impact sourcing decisions and restrict certain sources of supplies and services, although these rules no longer relate directly to country of origin.[179]

Contractors (and their subcontractors) also are subject to U.S. economic sanctions regulations that are incorporated by reference in the FAR and that flow down through the entire supply chain.[180] Finally, contractors that participate in the Foreign Military Financing Program should be aware that the U.S. Government will generally finance only U.S. content.[181]

■ Export Controls

There can be significant compliance risk associated with U.S. export control laws, which are predominantly outside the FAR system.

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,[182] and the Export Administration Regulations (EAR), administered by the Commerce Department.[183] In general, the ITAR imposes defense-related export controls, whereas the EAR primarily imposes dual-use-related controls (and, as a result of recent reform efforts, some military items).[184] A wide variety of activities can constitute exports, including shipping items from the United States, personally carrying controlled technical data out of the United States on an electronic device, transmitting information electronically, allowing access by "foreign persons" (a term defined in the ITAR and EAR) to company networks, directories, etc. with controlled technology, releasing controlled data during spoken conversations, and transferring hardware or controlled technology to foreign persons within the United States (known as "deemed exports").

In the procurement context, an export can include sharing U.S.-controlled technical data with actual or potential suppliers that employ foreign persons, transmitting such data to foreign 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 U.S. jurisdiction is shipped or transmitted from one foreign country to another foreign country or to an unauthorized user in the same foreign country.

(1) *International Traffic in Arms Regulations (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.[185] The U.S. Munitions List (USML), published in the ITAR, sets forth 21 categories of controlled defense articles and defense services.[186]

"Defense articles" include hardware, technical data, and software, including incorporated parts and components, that are specifically (or "specially") designed, developed, configured, adapted, or modified for a military, space, or intelligence application and are not subject to the EAR (i.e., do not have a predominant civil application/performance equivalent).[187] Controlled technical data" is information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles, which may include drawings, design specifications, software, photographs, and work instructions.[188]

"Defense services" include the furnishing of assistance 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.[189]

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 (subject to special license exemptions for certain close allies), or to a foreign person. Formal export licenses are generally required for hardware. Exports of technical data and services are typically authorized pursuant to "technical assistance agreements" (TAAs)[190] or "manufacturing license agreements" (MLAs).[191]

Companies involved with ITAR defense articles and services are usually obligated to register with the DDTC, even if they merely manufacture ITAR-controlled defense articles in the United States (rather than export those articles).[192] Registration also is required for brokering activities related to defense articles and defense services, such as facilitating foreign sales. Registration, however, does not independently provide any export authorization.[193]

(2) *Export Administration Regulations (EAR)*. Almost everything that is not subject to the ITAR is likely to be subject to the EAR.[194] 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).[195] Dual-use items are commodities, software, or technology that have both a commercial and military application. Unlike the ITAR, which control exports to essentially all countries, 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. In certain circumstances, the EAR may restrict the application abroad of technical assistance (e.g., training) by a U.S. person involving certain controlled technology or specific end uses (e.g., chemical and biological weapons).

There are several exceptions that affect Government contractors when they are performing work for the United States or an allied Government. These include 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).

(3) *ITAR and EAR Supply Chain Compliance Considerations.* Contractors need to be aware of the ITAR at all stages of an opportunity, whether for a U.S. agency customer, a foreign government (either as a direct commercial sale or as part of the Foreign Military Sales program), or a U.S. or foreign prime contractor. ITAR compliance is particularly complex to manage with a multi-layered supply chain where 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[196] that specifies the need to comply with export controls (referring to the EAR and ITAR by name) and implies that a violation of export control regulation may be considered a contract violation. In a domestic supply chain setting supporting the U.S. customer, prime contractors should consider creating their own "bespoke" export control clauses that supplement the DFARS provision. This is important with respect to domestic subcontractors and suppliers as well as foreign entities. Foreign suppliers and subcontractors also may need to enter into TAAs separate and apart from their main subcontracts, to receive export-controlled technical data and collaborate with U.S. entities higher up the supply chain.

Contractors and subcontractors should be mindful of the possible interplay between export control, voluntary disclosure regimes, and an August 2015 DFARS interim rule that requires that cyber-incidents involving export-controlled information be reported to the DOD. These requirements reach the supply chain by virtue of a flowdown clause, which requires that cyber-incidents be reported to both the prime contractor and the DOD.[197]

■ Foreign Corrupt Practices Act

Government contractors performing work abroad face substantial risks under the U.S. Foreign Corrupt Practices Act (FCPA)[198] and the anti-corruption laws of relevant foreign jurisdictions. This may seem counterintuitive because the FCPA deals with bribes to "foreign" officials whereas U.S. Government contractors work with U.S. Government officials. However, even when performing a U.S. Government contract, there are many opportunities for FCPA violations, particularly through the supply chain.

The FCPA criminalizes the bribery of "foreign officials" 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.[199]

The FCPA prohibits not only direct bribes but also the making, authorizing, offering, or promising of payments to "any person"—including third parties such as agents, representatives, subcontractors and suppliers—with knowledge or reason to believe that the payments will be passed through to persons covered by the statute.[200] In addition, the FCPA obligates U.S. and foreign companies with publicly traded securities in the United States to follow 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.[201]

The FCPA presents some unique risks. 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 important U.S. allies) where public corruption may be common. It covers U.S. companies, citizens, and permanent residents (by virtue of their nationality), "issuers" of publicly traded securities in the United States and, in certain circumstances, non-U.S. nationals and non-U.S. corporations where some act in furtherance of the prohibited payment occurs in the United States.[202]

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 that may lack transparency. Accordingly, a significant source of risk under the FCPA for U.S. and other government contractors is the use and control (or lack thereof) of third parties in the course of a company's business dealings. Although a contractor may not be the one making a particular payment, or the payment made by the contractor may be made to a third party rather than a "foreign official," enforcement agencies might attempt to rely on theories of vicarious liability to impute liability to the contractor.

To protect against this risk, Raytheon's International Terms and Conditions of Purchase (TC-004) requires suppliers to cooperate with, and provide assistance to, Raytheon in implementing adequate due diligence procedures in connection with the supplier's selection and retention of consultants and subcontractors. In addition, the supplier must have such consultant and subcontractor provide a "Questionnaire and Certification form" and any other documentation reasonably required by Raytheon for review.

Third-party FCPA risks occur most frequently when contracting with a foreign government, either through direct contract sales or foreign military sales, because agents/representatives and local partners may be required as part of the direct contracting regime of the foreign government. However, the past few years have seen the rise of U.S. Government service contracts being performed abroad, particularly in support of contingency operations. These are also high risk for Government contractors in light of the numerous corruption risks when using customs brokers, security contractors, etc. This is true not only for U.S. prime contractors but also for subcontractors. Service contracts also provide many opportunities for third parties to interact with foreign governments, such as customs, tax, and immigration officials.

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

(1) *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 other 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 U.S. Department of Justice and the Securities Exchange Commission published a guide on these topics in 2012 that contractor's should consider reviewing.[203]

(2) *Ensure 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. In light of the FCPA's accounting requirements, this is particularly important for issuers.

(3) *Effective policy implementation.* U.S. enforcement authorities continue to place emphasis on the communication and training 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 or 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 knowledgeable company personnel are available to provide real-time guidance when questions arise is also an important component of an effective FCPA compliance program.

(4) *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 reporting when FCPA concerns arise, and investigate and address those concerns, are less likely to encounter problems in the future. Companies also should periodically test their FCPA compliance measures, through internal audit and outside counsel, and encourage (or mandate) that suppliers have similar review mechanisms.

Although these compliance 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, reduce the likelihood of violations, and show good faith due diligence if violations occur. This will help protect the value of the company's overseas business as it shifts its attention to non-U.S. 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 Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, which was adopted in 1998,[204] a number of other countries have implemented, updated, and more rigorously enforced transnational anticorruption laws. When a U.S. contractor works abroad, it must be mindful of these third-country national and local laws. For example, the United Kingdom's Bribery Act, passed in 2010,[205] imposes criminal sanctions upon bribery and is a qualifying statute under the OECD Convention. Although there has been little enforcement of the Act to date, it appears to have a more expansive jurisdictional reach than the FCPA and addresses actions not subject to the FCPA, such as 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.[206] Such a defense may protect them against liability in the event improper payments are made by "bad apples" associated with the company.

The UK Bribery Act's "adequate procedures" defense highlights the importance of implementing effective compliance policies when companies operate abroad. Those policies are important to protect companies from FCPA liability in the United States, Bribery Act liability in the United Kingdom, and transnational bribery laws of other major trading nations, such as Canada and Germany, which have stepped up their enforcement efforts.

■ Combating Trafficking In Persons

The issue of trafficking in persons has become highly visible and as a result has garnered increased attention. Throughout the world, people are being exploited through trafficking—some could be in your supply chain.[207] In response, the U.S. has adopted a "zero tolerance" policy prohibiting trafficking in persons,[208] and addresses the problem through a variety of laws and regulations, including the Trafficking Victims' Protection Act of 2000 (TVPA), several later laws,[209] and the FAR.

Although some FAR trafficking in persons requirements apply principally to contracts performed outside the U.S., many of the rules apply to contracts performed in the United States as well.[210] Government contractors (and subcontractors) must comply with applicable federal legislation and regulations issued to combat trafficking in persons, including in particular the "Combating Trafficking in Persons" (CTIP) rules found in the FAR.[211]

The CTIP rules address trafficking in persons in three areas that are important to managing supply chains:

(1) They prohibit a range of activities related to trafficking in persons that are applicable

to all Government contracts and subcontracts, including COTS items;

(2) They create an expanded reporting and enforcement mechanism applicable to all contractors; and

(3) They impose a broad set of compliance plan, due diligence and certification requirements for overseas contracts and subcontracts valued over $500,000.

(1) *Prohibitions Applicable to All Contracts.* For more than a decade, a CTIP FAR clause has included basic prohibitions against engaging in trafficking in persons. Prohibited activities include (a) engaging in severe forms of trafficking in persons, including using force or the threat of force in hiring or 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.[212] The newly prohibited practices include simple prohibitions on destroying, concealing, confiscating or otherwise denying access to the employee's identity or immigration documents; as well as more complex prohibitions, such as those relating to denial of payment for return transportation. These require a careful analysis of related rules for protecting employee victims and witnesses in trafficking investigations.[213]

(2) *Awareness and Disclosure Commitments.* In addition to these prohibited activities, the CTIP FAR clause commits all 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 and subcontractors to notify the Government when they receive "credible information" that a contractor employee, subcontractor, subcontractor employee, or their agent has violated the CTIP regulations.[214] The CTIP FAR clause also commits the contractor to provide "full cooperation" with Government CTIP investigations and audits, which includes commitments to (a) 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, (b) provide timely and complete responses to auditor's and investigator's requests for documents, (c) provide reasonable access to facilities and staff to facilitate federal audits and investigations, (d) protect employees suspected of being victims of trafficking or witnesses, and (e) refrain from hindering or preventing employees from cooperating with U.S. Government authorities.[215]

The CTIP FAR clause is a mandatory flow down clause for all covered contracts.[216] Thus, subcontractors must be knowledgeable about these prohibitions and monitor their own supply chains for compliance. This may not be simple; contractors (and subcontractors) that try to monitor and enforce these requirements may encounter resistance from some suppliers, who are not subject to the prime contractor's control, especially if they are competitors in other areas.

(3) *Requirements for Overseas Contracts Valued Over $500,000.* Contracts and subcontracts (except COTS) that are to be performed outside the U.S. and have an estimated value exceeding $500,000 have additional requirements.[217] These additional requirements include having a compliance plan for preventing, monitoring, and detecting trafficking in persons, engaging in due diligence to determine potential violations in the contractor's supply chain, and obtaining "no violation" certifications from the supply chain. While the CTIP rule identifies certain minimum elements for this compliance plan,[218] the discussion in its regulatory history makes it clear that the compliance plan is not a one-size-fits-all prescription. Rather, the compliance plan must be appropriate to (a) the size and complexity of the contract and (b) the nature and scope of the activities to be performed under the contract, including the number of non-U.S. citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking.[219]

In addition to maintaining its own CTIP compliance plan, the contractor must make one of the following certifications to the CO annually after receiving an award and "[a]fter having conducted due diligence":[220]

> (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.

Before making this certification, the prime contractor must conduct a due diligence review of its supply chain and investigate whether its agents and subcontractors have engaged in prohibited practices.[221] (For example, Raytheon has included such CTIP certifications in its CR-003 Certification template referenced above.) The prime contractor's monitoring efforts should be based on the risk of trafficking in persons related to the particular product or service being acquired. An important consideration is whether or not the prime contractor has direct access to a work site. Where a prime contractor has direct access, it may be expected to look for signs of trafficking in persons at the workplace and, if housing is provided, inspect the housing conditions. Where the employees and subcontractors are geographically distant, or for lower tier subcontractors, the prime must review the plans and certifications of its subcontractors to ensure they include adequate monitoring procedures and should compare this information to public audits and other trafficking in persons data available.[222]

Most importantly, these minimum commitments must be flowed down to all subcontracts and contracts with agents involving non-COTS subcontracts for which the overseas portion exceeds $500,000.[223]

The CTIP rules incentivize companies to engage in risk assessment and due diligence prior to and during contract performance and to maintain an effective due diligence and risk assessment program that includes effective training, monitoring, auditing, and reporting.

Further Regulation Of The Supply Chain

This Briefing Paper has examined supply chain risk management and compliance issues facing Government contractors and discussed many of the current concerns that companies must address in addressing supply chain risk management and compliance. Contractors, however, should expect that new laws and implementing regulations will continue to affect supply chain risk management and compliance. Anticipated additional rulemaking in the areas of organizational conflicts of interest, counterfeit parts, and implementation of the Fair Pay and Safe Workplaces Executive Order[224]—to name just a few topics—will affect the supply chain. Cybersecurity issues and restrictions in sourcing from certain countries will also continue to receive attention. These likely developments highlight the need for Government contractors to keep abreast of new legal and regulatory developments and to consider frequent reviews and, as necessary, revisions of policies, procedures, standard terms and conditions of purchase, and standard agreements.

GUIDELINES

These *Guidelines* are intended to assist you in understanding the legal issues Government contractors face related to supply chain risk management and compliance. They are not, however, a substitute for professional advice and representation in any particular situation.

1. Recognize that supply chain risk management deserves appropriate senior management attention. Supply chain issues can affect the company in many ways, including its legal exposure, past performance ratings, and reputation.

2. Be aware that the supply chain function should be viewed as a compliance function and it should be staffed and managed accordingly. This function does more than issue purchase orders. It must vet suppliers, negotiate tailored terms and conditions, and engage in adequate oversight of suppliers.

3. Remember that the training of supply chain personnel is essential. This is a rapidly changing area, and it is vital that the supply chain function stay on top of new initiatives and rules. Some rules expressly require training of suppliers and third parties.

4. Bear in mind that standard terms and agreements (that can be tailored and adopted) increase efficiency and can reduce the time and effort needed to "reinvent the wheel" in every subcontract negotiation. Consider the benefits of placing standard terms and agreements on the company's website.

5. Use technology to make the function more effective and integrate supply chain information with other company functions.

6. Understand and exploit the benefit of alliances and team arrangements with key suppliers. These alliances are an asset and need to be managed to preserve their value.

7. Consider the benefit of close integration of the supply chain and prime contracting functions. This will facilitate a seamless alignment of prime contract requirements with flowdown provisions in the subcontracts or purchase orders.

8. Regularly review policies and procedures and standard terms and agreements in light of new rules and regulations. Consider an outside review by experts on a regular basis to ensure that important developments have not been missed.

9. Ensure that you have access to necessary resources, including experts, to assist in addressing supply chain issues and, where needed, conducting investigations. Outside resources may be helpful in vetting new suppliers, particularly when the supplier is located outside the U.S. and is not known to the company.

10. Pay particular attention to the laws and regulations that address international suppliers in your supply chain. You may be using a global supply chain in support of domestic U.S. programs, as well as in support contracts being performed overseas. This makes compliance with global trade laws and regulations a necessity.

11. Remember that negotiating leverage between prime and subcontractor may change upon award. Consider whether key issues should be addressed in teaming agreements or deferred to subcontract negotiations.

12. Keep in mind that prime contractors and subcontractors may have different goals. Understand them and take them into account.

13. Do not be trapped by "general policy." The specific situation may require flexibility. Many positions are not "right" or "wrong," but reflect differing goals and leverage.

★ REFERENCES ★

1/ Morris, "Why Your Company Needs a Chief Supply Chain Officer, Fortune (Sept. 10, 2015), http://fortune.com/2015/09/10/chief-supply-chain-officer/.

2/ Morris, "Why Your Company Needs a Chief Supply Chain Officer, Fortune (Sept. 10, 2015), http://fortune.com/2015/09/10/chief-supply-chain-officer/.

3/ Morris, "Why Your Company Needs a Chief Supply Chain Officer, Fortune (Sept. 10, 2015), http://fortune.com/2015/09/10/chief-supply-chain-officer/.

4/ See FAR subpt. 44.3; DFARS subpt. 244.3.

5/ FAR 3.1001.

6/ 80 Fed. Reg. 67,244, 67,250 (Oct. 30, 2015), (citation omitted).

7/ 80 Fed. Reg. 30,548, 30,553 (May 28, 2015); see Mutek, "Feature Comment: Proposed Fair Pay and Safe Workplaces Rule and Guidance—We May Have Come a Long Way Since 2001, But Compliance and 'Blacklisting' Concerns Remain," 57 GC ¶ 189.

8/ That is why Steptoe & Johnson, LLP created its Supply Chain Toolkit, available at http://www.steptoe.com/f-585.html. This Briefing Paper draws from that toolkit.

9/ Available at http://www.oecd.org/corruption/oecd-foreign-bribery-report-9789264226616-en.htm.

10/ DFARS 246.870, 252.246-7007.

11/ FAR subpt. 22.17, 52.222-50.

12/ 80 Fed. Reg. 67,244, 67,250 (Oct. 30, 2015) (citation omitted).

13/ DFARS 239.7305.

14/ ICD 731 (Dec. 7, 2013), available at http://fas.org/irp/dni/icd/icd-731.pdf.

15/ FAR 44.101.

16/ FAR 44.302.

17/ FAR 44.301.

18/ See 76 Fed. Reg. 28,856 (May 18, 2011) (interim rule); 77 Fed. Reg. 11,355 (Feb. 24, 2012) (final rule).

19/ DFARS subpt. 242.70, 252.242–7005.

20/ DFARS subpt. 242.70.

21/ DFARS 252.244-7001(c).

22/ DFARS 252.244-7001(a).

23/ FAR 44.202-2, 44.303.

24/ FAR 44.202-2.

25/ 31 U.S.C.A. § 3729–3733.

26/ 31 U.S.C.A. § 3729(a)(1).

27/ 31 U.S.C.A. § 3729(a)(1).

28/ 31 U.S.C.A. § 3729(b)(1).

29/ See Holt & Klass, "Implied Certification Under the False Claims Act," 41 Pub. Cont. L.J. 1 (2011); Mitchell, Abbott & Orozco, "Implied Certification Under the False Claims Act," Briefing Papers No. 11-4 (Mar. 2011).

30/ https://www.sam.gov/portal/SAM/#1

31/ FAR 9.104-4(a).

32/ FAR 3.303.

33/ FAR 9.604.

34/ FAR 9.103(a).

35/ FAR 9.104-4(a).

36/ FAR 9.104-4(b).

37/ FAR 9.104-1.

38/ FAR 52.209-6.

39/ FAR 52.209-6.

40/ FAR 15.304(c).

41/ FAR subpt. 42.15.

42/ More information is available at https://www.sam.gov/portal/SAM/#1.

43/ FAR 9.104-6(a).

44/ FAR 52.244-5.

45/ See Koehler, "Teaming Agreements: The Proverbial 'Wolf in Sheep's Clothing,'" Briefing Papers No. 14-6 (May 2014).

46/ FAR subpt. 9.6.

47/ FAR 9.604.

48/ FAR 3.303(c)(7).

49/ See FAR subpt. 9.5.

50/ See FAR subpt. 3.11; see also Szeliga &Turner, "Preventing Personal Conflicts of Interest Among Contractor Employees Performing Acquisition Support Services," Briefing Papers No. 12-4 (Mar. 2012).

51/ See FAR 9.505-1 to 9.505-4, 3.1103, 3.1104.

52/ See FAR 9.504.

53/ Fed. Trade Comm'n & U.S. Dep't Of Justice, Antitrust Guidelines for Collaborations Among Competitors (Apr. 2000), available at http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf.

54/ Available at http://www.raytheon.com/rtnwcm/groups/corporate/documents/image/rtn_279815.pdf.

55/ See U.S. Gov't Accountability Office, GAO-15-423R, Department of Defense: Acquisition Rulemaking Practices 2 (Apr. 17, 2015).

56/ See U.S. Gov't Accountability Office, GAO-15-423R, Department of Defense: Acquisition Rulemaking Practices 2 (Apr. 17, 2015).

57/ See http://www.raytheon.com/suppliers/supplier_resources/.

58/ 22 C.F.R. pt. 130.

59/ Available at http://www.raytheon.com/rtnwcm/groups/corporate/documents/image/rtn_279815.pdf.

60/ 22 C.F.R pts.120–130.

61/ 15 C.F.R. pts. 730–774.

62/ See http://www.raytheon.com/suppliers/supplier_resources/.

63/ See http://www.dii.org/.

64/ United States Sentencing Comm'n, Guidelines Manual, ch.8, pt. B (Nov. 201), available at http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2015/GLMFull.pdf.

65/ FAR 3.1004, 52.203-13.

66/ FAR 52.203-13. See generally Chierichella & Casino, "Compulsory Confession Without Absolution: Complying With the FAR Mandatory Disclosure Rule," Briefing Papers No. 15-10 (Sept. 2015).

67/ 41 U.S.C.A. ch. 87.

68/ FAR 3.502-2(g).

69/ FAR 3.502-1.

70/ FAR 52.203-13(a), (b)(3).

71/ FAR 52.203-13(c)(1)(ii).

72/ FAR 52.203-13(d).

73/ 73 Fed. Reg. 67,064, 67,084 (Nov. 12, 2008).

74/ Vanek & Tibbets, "Counterfeit Electronic Parts—The DFARS Rule and the Expanding Reporting Requirements for Nonconforming Parts," Briefing Papers No. 14-11, at 1 (Oct. 2014).

75/ National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 818, 125 Stat. 1298, 1493 (2011); National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 833, 126 Stat. 1632, 1844 (2013).

76/ 79 Fed. Reg. 26,092 (May 6, 2014) (adding DFARS 246.870).

77/ DFARS 252.246-7007.

78/ DFARS 252.246-7007.

79/ DFARS 246.870-3.

80/ DFARS 202.101, 252.246-7007(a).

81/ DFARS 252.246-7007(c).

82/ 79 Fed. Reg. 26,092, 26,100 (May 6, 2014).

83/ DFARS 231.205-71.

84/ Federal Acquisition Regulation; Expanded Reporting of Nonconforming Items (FAR Case 2013–002), 79 Fed. Reg. 33,164 (June 10, 2014) (proposed rule); see also Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts—Further Implementation (DFARS Case 2014–D005), 80 Fed. Reg. 56,939 (Sept. 21, 2015) (proposed rule).

85/ 78 Fed. Reg. 69,268 (Nov. 18, 2013).

86/ DFARS subpt. 239.73 ("Requirements for Information Relating to Supply Chain Risk").

87/ 80 Fed. Reg. 67,244 (Oct. 30, 2015).

88/ Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111–383, § 806(e)(4), 124 Stat. 4137, 4260 (2011); 80 Fed. Reg. at 67,250.

89/ 80 Fed. Reg. 67,244.

90/ 80 Fed. Reg. at 67,249.

91/ 80 Fed. Reg. 51,739 (Aug. 26, 2015) (amending DFARS subpt. 204.73 to implement National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 941, 126 Stat. 1632, 1889 (2013); National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 1632, 128 Stat. 3292, 3638 (2015)).

92/ 80 Fed. Reg. 51,739.

93/ DFARS 252.204-7008. Note that an interim rule published at 80 Fed. Reg. 81,472 (Dec. 30, 2015) after preparation of this Briefing Paper provides an additional year to implement the NIST standards.

94/ DFARS 252.204-7012.

95/ DFARS 252.204-7009

96/ DFARS 252.204-7008.

97/ DFARS 252.204-7008(d).

98/ DFARS 204.7304(a).

99/ ICD 731 (Dec. 7, 2013), available at http://fas.org/irp/dni/icd/icd-731.pdf.

100/ DFARS 239.7305.

101/ Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, § 516, 127 Stat 198, 272–73 (2013).

102/ DFARS 252.227-7013, 252.227-7014; FAR 27.401.

103/ DFARS 227.7103-4(a), 227.7203-4(a); FAR 52.227-14(b)(2).

104/ DFARS 227.7103-3(b), 227.7103-10(a), 227.7203-3, 227.7203-10(a), 252.227-7017.

105/ FAR 52.227-15.

106/ FAR 52.227-14(g) (Alt. II or Alt. III); DFARS 252.227-7013(f), 252.227-7014(f).

107/ FAR 27.404-5; DFARS 227.7103-10(c), 227.7203-10(c).

108/ DFARS 227.7103-11, 227.7203-11, 252.227-7013(g), 252.227-7014(g), 252.227-7019(b), 252.227 7037(c).

109/ DFARS 227.7103-8, 227.7203-8, 252.227-7026 (delivery), 252.227-7027 (ordering); FAR 27.406-2(b), 52.227-16.

110/ DFARS 227.7102-1, 252.227-7015.

111/ DFARS 227.7202-1(c), 227.7202-3.

112/ DFARS 227.7102-3, 227.7102-4(c), 252.227-7015(b)(1)(i), (d).

113/ FAR 12.211.

114/ FAR 12.212, 27.405-3.

115/ FAR 52.227-19.

116/ DFARS 227.7103-15(c), 227.7203-15(c), 252.227-7013(k), 252.227-7014(k), 252.227-7019(i) ("Validation of Asserted Restrictions—Computer Software"), 252.227-7037 (Validation of Restrictive Markings on Technical Data").

117/ DFARS 252.227-7013(k), 252.227-7014(k).

118/ DFARS 227.7103-15(d), 227.7203-15(d).

119/ DFARS 252.227-7013(k)(1), 252.227-7014(k)(3); see also DFARS 252.227-7017(c).

120/ DFARS 227.7103-15, 227.7203-15.

121/ DFARS 252.227-7013(k)(3).

122/ FAR 52.227-14(h).

123/ FAR 52.227-14(h).

124/ DFARS 227.7102-3(a).

125/ FAR 52.227-19.

126/ FAR 52.227-11; DFARS 252.227-7038.

127/ FAR 52.227-11; DFARS 252.227-7038.

128/ FAR 52.227-11; DFARS 252.227-7038.

129/ DFARS 252.227-7038(l).

130/ FAR 52.227-11(k).

131/ 28 U.S.C.A. § 1498 (Patent and copyright cases).

132/ FAR 52.227-1.

133/ FAR 52.227-1, Alt I.

134/ 28 U.S.C.A. § 1498 (Patent and copyright cases).

135/ FAR 52.227-3.

136/ See generally Meagher & Bareis, "The Freedom of Information Act," Briefing Papers No. 10-12 (Nov. 2010).

137/ Small Business Jobs Act of 2010, Pub. L. No. 111-240, § 1341, 124 Stat. 2504, 2543 (2010) (adding 15 U.S.C.A. § 632(w)).

138/ 15 U.S.C.A. § 632(w)(2).

139/ 15 U.S.C.A. § 632(w)(2).

140/ 15 U.S.C.A. § 645(d).

141/ 31 U.S.C.A. 3729–3733; 18 U.S.C.A §§ 287, 1001.

142/ 31 U.S.C.A. §§ 3801–3812.

143/ 31 U.S.C.A. 3729.

144/ FAR 19.708(b), 52.219-9.

145/ FAR 19.708.

146/ FAR 52.219-9(k).

147/ FAR 19.704(d), 52.219-9(g).

148/ FAR 19.704(a), 52.219-9(c).

149/ FAR 19.704(a), 52.219-9(l).

150/ FAR 19.704(b), 52.219-9(f).

151/ FAR 19.704(b).

152/ FAR 19.704(a), 52.219-9(d).

153/ FAR 52.219-9(k), 52.219-16; 15 U.S.C.A. § 637(d)(4)(F).

154/ FAR 15.304; DFARS 215.304; 15 U.S.C.A. § 637(d)(4)(G).

155/ Irwin & Rathbone, "Managing International Regulatory Risk in the Government Contract Supply Chain," Briefing Papers No. 11-6 (May 2011).

156/ 41 U.S.C.A. §§ 8302–8305.

157/ 19 U.S.C.A. § 2501 et seq.

158/ FAR 25.101(a).

159/ FAR 25.003.

160/ FAR 12.505(a), 25.101(a).

161/ FAR 25.103, 25.104.

162/ FAR 25.103(e).

163/ DFARS 252.225-7000, 252.225-7001.

164/ FAR subpt. 25.4.

165/ FAR 25.003.

166/ FAR 25.402. Note that calendar years 2016 and 2017, these thresholds are $191,000 and $7,358,000 respectively. 80 Fed. Reg. 77,694 (Dec. 15, 2015).

167/ FAR 25.401.

168/ FAR 25.502(b)(3).

169/ DFARS 252.225-7021.

170/ FAR 25.003; DFARS 252.225-7021(a).

171/ FAR 25.003; DFARS 252.225-7021(a).

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

173/ See United States ex rel. Folliard v. Government Acquisitions, Inc., 764 F.3d 19 (D.C. Cir. 2014).

174/ FAR 52.225-6.

175/ FAR 52.225-2.

176/ See FAR subpt. 9.4.

177/ DFARS 225.7002.

178/ Pub. L. No. 111-5, § 1605, 123 Stat. 115, 303 (2009).

179/ See 22 C.F.R. pt. 228.

180/ FAR 52.225-13 ("Restrictions on Certain Foreign Purchases").

181/ See Defense Security Cooperation Agency, Guidelines for Foreign Military Financing of Direct Commercial Contracts (Aug. 2009).

182/ 22 C.F.R pts.120–130.

183/ 15 C.F.R. pts. 730–774.

184/ See generally Baj, Cook, Hayes, Irwin et al., "Export Control Reform: Implementation & Implications," Briefing Papers No. 14-13 (Dec. 2014).

185/ 22 C.F.R pts.120–130.

186/ 22 C.F.R. § 121.1.

187/ 22 C.F.R. § 120.3, 120.6.

188/ 22 C.F.R. § 120.10.

189/ 22 C.F.R. § 120.9.

190/ 22 C.F.R. § 120.22.

191/ 22 C.F.R. § 120.21.

192/ 22 C.F.R. pt. 122.

193/ 22 C.F.R. pt. 129.

194/ 15 C.F.R. pts. 730–774.

195/ 15 C.F.R. Pt. 774, supp. 1.

196/ DFARS 225.7901-3.

197/ 80 Fed. Reg. 51,739 (Aug. 26, 2015) (amending DFARS subpt. 204.73).

198/ 15 U.S.C.A. § 78dd-1 et seq. See generally Williams, Caccia, Volkmar & Sharma, "The Foreign Corrupt Practices Act & Unique Risks For Government Contractors," Briefing Papers. No. 14-12 (Nov. 2014).

199/ 15 U.S.C.A. §§ 78dd-1(a), (f)(1), 78dd-2(a), (h)(2), 78dd-3(a), (f)(2).

200/ 15 U.S.C.A. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a).

201/ 15 U.S.C.A. § 78m(b)(2).

202/ 15 U.S.C.A. § 78dd-1 et seq.

203/ See U.S. Dep't of Justice Criminal Div. & Secs. & Exch. Comm'n Enforcement Div., A Resource Guide to the U.S. Foreign Corrupt Practices Act 4 (Nov. 14, 2012), available at http://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

204/ See http://www.oecd.org/corruption/oecdantibriberyconvention.htm.

205/ Bribery Act, 2010, c. 23 (Eng.). For text of the act, see http:// www.legislation.gov.uk/ukpga/2010/23/contents; see also UK Ministry of Justice, The Bribery Act 2010: Guidance (Mar. 2011), available at http:// www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

206/ Bribery Act, 2010, c. 23, § 7 (Eng.).

207/ See Johnson Jr., "Business Lawyers Are in a Unique Position To Help Their Clients Identify Supply-Chain Risks Involving Labor Trafficking and Child Labor," 70 Bus. Law. 1083 (Fall 2015).

208/ FAR 22.1703.

209/ See Victims of Trafficking and Violence Protection Act of 2000, 22 U.S.C.A. §§ 7101-7112; see also Trafficking Victims Protection Reauthorization Act of 2003, Pub. L. No. 108-193, 117 Stat. 2875 (2003); Trafficking Victims Protection Reauthorization Act of 2005, Pub. L. No. 109-164, 119 Stat. 3558 (2006); William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Pub. L. No. 110-457, 122 Stat. 5044 (2008).

210/ See Navarre & Mutek, "Final Trafficking in Persons Rule Creates a New Compliance Component for U.S. Government Contractors," 57 GC ¶ 74; see also Ittig, Witten & Fitzpatrick, "The New Anti-Trafficking Rules and What They Mean for Government Contractors and Subcontractors," Briefing Papers No.15-11 (Oct. 2015).

211/ FAR subpt. 22.17, 52.222-50.

212/ 80 Fed. Reg. 4967 (Jan. 29, 2015) (codified at FAR pts. 1, 2, 9, 12, 22, 42, and 52).

213/ FAR 52.222-50.

214/ FAR 52.222-50(d).

215/ FAR 52.222-50(g).

216/ FAR 52.222-50(i).

217/ FAR 52.222-50(h).

218/ FAR 52.222-50(h)(3).

219/ FAR 52.222-50(h)(2).

220/ FAR 52.222-50(h)(5).

221/ FAR 52.222-50(h)(5).

222/ 80 Fed. Reg. 4967, 4976 (Jan. 29, 2015).

223/ FAR 52.222-50(i).

224/ See 80 Fed. Reg. 30,548 (May 28, 2015) (proposed rule implementing Exec. Order No. 13673, Fair Pay and Safe Workplaces (July 31, 2014), 79 Fed. Reg. 45,309 (Aug. 5, 2014)).