THOMSON REUTERS
Westlaw®

Q&A: Akin Gump's Angela Styles on current trends in government contracting and issues impacting contractors in today's environment

By Angela Styles, *Esq., Akin Gump**

APRIL 22, 2019

Thomson Reuters: What are the most significant issues in federal contracting today?

Angela Styles: Federal contracting faces four interrelated yet often inconsistent policy and legal issues: (1) deregulation of the contracting system with the goal of attracting the best commercial providers and lowering the cost of doing business for contractors and the taxpayer; (2) the replacement of legacy information technology systems and the need to access critical new technologies, (3) an increased need to harden and protect cybersystems; and (4) the federal government's lack of confidence in the contracting supply chain.

> Increasingly, however, real innovation is happening at companies, both small and large, that have little desire to be federal contractors.

Through initiatives like Congress' mandated Section 809 panel review of Department of Defense regulations, the rapidly progressing e-commerce platform at the General Services Administration, percolating changes to the Cost Accountings Standards, and the vastly increased use of federal statutory "other transactions authority" by DOD for unique contracting arrangements, the federal government is driving hard to streamline the contracting system and find fast and easy mechanisms for accessing commercial products and new technologies with few legal or contractual restraints.

On the other hand, the federal government and its providers are under extraordinary pressure to fend off increased cybervulnerabilities, forcing the government to significantly increase regulatory cyber-requirements and oversight of contractors and subcontractors. Similarly, weaknesses in the supply chain threaten safety, and the government has responded with regulations and increased oversight of federal contractors by the executive and legislative branches.

TR: What steps is the government taking to upgrade technology and legacy IT systems? And how is the government accessing new technologies?

AS: First and foremost, DOD and the Department of Homeland Security have long recognized the need for cutting-edge technologies to equip our warfighters and protect the country. Increasingly, however, real innovation is happening at companies, both small and large, that have little desire to be federal contractors.

Be it the intellectual property provisions that can give the federal government and other companies rights to your technology, cost accounting requirements or the simple cost of a contracting compliance program, many of the innovators have steered far clear of federal contracting.

To attract these companies to the table, DOD has worked hard to use nontraditional procurement vehicles through OTA (authority allowing legally binding agreements between the government and private sector businesses or universities that are not subject to the Federal Acquisition Regulation) to speed up the acquisition process and provide opportunities for greater engagement and outreach through entities like the Defense Innovation Unit in Silicon Valley and the Army Futures Command in Austin, Texas.

TR: What can the private sector company or a university do to engage or participate in providing and developing new technologies? What should federal contractors or potential contractors watch out for when the government uses unique procurement vehicles like an OTA?

AS: Do your homework and engage. Be it with the Army Futures Command, the Defense Innovation Unit or one of the Department of Energy's National Research Labs, most companies find that the government's door opens when they knock. The National Labs in particular are an untapped source of innovation, with extraordinary user facilities and scientists in every field from quantum and exascale computing to propellants and advanced photon source research.

Indeed, technology transfer to the private sectors is one of the primary missions of the labs. Such transfers may be undertaken in a

variety of ways, including through lab partnering agreements such as cooperative research and development agreements, work-for-others agreements, user facility agreements and the licensing of intellectual property.

One of the best places to examine how a private company or university might best engage with the federal government is the Office of Technology Transitions at the Department of Energy. The department's website is https://bit.ly/2Dv0klQ.

> The federal government and its providers are under extraordinary pressure to fend off increased cyber vulnerabilities.

DOD and DHS are also actively using alternative contracting vehicles, like agreements using OTA, to bring new companies to the table and collaborate with more traditional federal contractors. On the surface, OTAs are a terrific way to attract new companies and technologies to the table. Unlike FAR-based contracts, OTA agreements have a limited amount of constraints — there are no required certifications, no cyber-requirements, no termination-for-convenience clauses, no Truth in Negotiations Act requirements, no cost accounting standards and no intellectual property clauses transferring rights away from a contractor.

However, companies signing OTAs, participating in OTA consortiums or subcontracting on OTAs should bear in mind that these agreements are not without risk that runs the spectrum from fraud to the failure to carefully remove clauses that are not required. In many instances, the federal government and prime OTA agreement holders continue to include intellectual property clauses and cost accounting clauses that are not required.

In addition, OTAs do not exempt you from complying with other laws, such as those on export control. Critically important, however, if you want to do more than research or make prototypes, with limited exceptions, you will need to make the leap from an OTA to FAR-based federal contracting for production contracts.

Under the FAR, contractors have to comply with the cybersecurity and supply chain requirements for federal contractors. Don't put yourself in a position during the performance of an OTA where you may not be able to meet cybersecurity requirements or you have difficulty finding a secure supply.

TR: What are the cybersecurity and supply chain requirements for federal contractors and subcontractors and when do they apply? Is the federal government simultaneously trying to regulate supply chains and cybersecurity and deregulate other areas?

AS: Cybersecurity. Currently, FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, mandates that any information system that "processes, stores, or transmits Federal contract information" must comply with a minimum of 15 security controls that are listed in that clause.

Agency-specific clauses also impose cybersecurity controls on contractors. The most widely discussed and well known is Defense Federal Acquisition Regulation Supplement 252.2047012, Safeguarding Covered Defense Information and Cyber Incident Reporting. This is also known as the 7012 clause.

DOD contractors and subcontractors that will possess, or that will use a third-party that will possess on their behalf, "covered defense information" are subject to the 7012 clause. Covered defense information is controlled unclassified information that is marked or collected, developed, received, transmitted, used or stored by the company in support of the performance of a contract.

> Beyond compliance with the FAR and the DFARS, contractors should be aware of agency-specific initiatives to require compliance with further cybersecurity-related requirements.

The 7012 clause requires a contractor or subcontractor to (1) implement the standards of National Institutes of Standards and Technology Special Publication 800-171; (2) rapidly report cybersecurity incidents within 72 hours of discovery; (3) assist DOD with damage assessments of cybersecurity incidents; and (4) flow down the 7012 clause to all subcontracts (except those involving commercial off the shelf, or COTS, items) that will receive, transmit or use CDI in the performance of the subcontract.

If a contractor subject to the 7012 clause is not already in compliance with the requirements of NIST SP 800-171 at the time of contract award, it must have a written system security plan and any associated plans of action and milestones, commonly referred to as POAMs, in place.

Additionally, the FAR Council will soon propose an amendment to the FAR that will implement additional requirements related to protection of controlled unclassified information. Contractors should expect issuance of a final FAR clause to that effect this year.

Beyond compliance with the FAR and the DFARS, contractors should be aware of agency-specific initiatives to require compliance with further cybersecurity-related requirements. In particular, in September 2018, the assistant secretary of

the Department of the Navy issued a memorandum titled "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks." The memorandum states that the Navy will soon require contractors to, among other things, deliver SSPs for approval by the government (the current 7012 clause only requires a contractor that has yet to implement the NIST 800-171 controls to have an SSP in place).

The memorandum also states that the Navy will impose new requirements that are not included in the 7012 clause, including the requirement that a contractor allow the Naval Criminal Investigative Services to install sensors on contractor systems if it identifies a vulnerability.

> There are great things happening in federal procurement, but for our system to continue to be world-class, we all have to participate.

Supply chain. Contractors are subject to a host of supply chain requirements, ranging from compliance with the FAR's anti-human trafficking clause (FAR 52.222-50 Combating Trafficking in Persons) to DFARS provisions related to detection of counterfeit parts (DFARS 252.246-7007 Contractor Counterfeit Electric Part Detection and Avoidance System and DFARS 252.246-7008 Sources of Electronic Parts).

In a nod to the cybersecurity threat that the government perceives through the use of products or services offered by certain foreign firms, the FY 2018 National Defense Authorization Act forbade every U.S. government agency from using any hardware, software or services developed or provided by Russia-based Kaspersky Lab and other related entities, and that prohibition is imposed on government contractors via FAR clause 52.204-23.

Further, the 2019 NDAA also included a provision, Section 889, banning federal agencies, federal contractors, or grant or loan recipients from contracting with (primarily) Huawei and rival ZTE, both of which are based in China, for telecommunications equipment and services.

TR: When do cybersecurity and supply chain requirements apply?

AS: The timing of when each of the aforementioned requirements applies to a contractor differs depending on the clause in question. For example, while a contractor generally must comply with DFARS clauses as of the time that it enters into a contract with an agency of the DOD, the 7012 clause will not apply to a contractor that will not receive or possess CDI pursuant to a contract, even if that contract includes the 7012 clause. Accordingly, while such a contractor is technically subject to the 7012 clause, the contractor is not required to implement the NIST 800-171 controls because it will not have CDI that requires protection.

TR: Is there simultaneous regulation and deregulation?

AS: Yes, absolutely, and this is most evident for commercial items. The cyber and supply chain clauses are applicable in many instances to commercial item contracts. If a contractor will be receiving covered information, the clauses will apply. Conflicting priorities are simultaneous, making it easier and harder for the federal government to access needed products and services.

TR: What is the risk of deregulation and will there be a move to easier procurement vehicles like OTAs?

AS: When you ease up on the rules and regulations, there always seem to be bad actors ready to take advantage. Every time there is a public sector contracting scandal, the statutes and regulations seem to tighten to prevent the problem from occurring again.

However, as the government attempts to regulate to guard against every potential case of fraud, waste or abuse, many of the best companies and innovators make a rational determination that the cost of compliance is too high. We are clearly at the point on the pendulum where the cost seems to be too high and the federal government is struggling to access what it needs to provide the best equipment for our warfighters and the best services to our citizens. As we swing back to a less regulated/less enforcement environment, fraud will likely increase again.

TR: What are the hardest areas of federal procurement to deregulate?

AS: For many years, the executive and legislative branches of government have chosen to use the federal procurement system to achieve goals that are not directly related to the product or service that is being purchased from the private sector.

So, for example, decades ago, Congress enacted legislation, known as the Buy American Act, requiring federal agencies to purchase only products manufactured in the United States. Similarly, there are statutes favoring the award of 23% of all federal contracts to U.S. small businesses.

Through executive order, the government has required a certain amount of paid leave for federal contractor employees and required companies to use the E-Verify system for immigration status confirmation for all contractor and subcontractor employees.

None of these statutes or regulations necessarily improve the quality of the product or service, but they are choices we made as a country to use our procurement system to influence certain behaviors and assist certain industries. These are unquestionably the hardest areas to deregulate.

TR: Do you have advice for federal contractors trying to navigate these seemingly conflicting priorities of the federal government?

AS: Be aware and participate. There are great things happening in federal procurement, but for our system to continue to be world-class, we all have to participate. The federal government has opened the door for engagement and deregulation. Over the past several years, federal agencies, with DOD, DHS and the General Services Administration often taking the lead, have held an unprecedented number of public meetings and issued many requests to engage early in the rulemaking process. While many people and companies may be hesitant to speak up, the only way to facilitate good change is for all voices to be heard.

On the other side of the coin, I would ask innovators and entrepreneurs to look to the many great things the federal government has to offer in terms of facilitating research and development. We are much better when the two sectors are working together and understand each other.

This article first appeared in the April 22, 2019, edition of Westlaw Journal Government Contracts.

ABOUT THE AUTHOR

Angela Styles is a partner at **Akin Gump** in Washington with a practice spanning nearly 25 years. She helps clients efficiently resolve federal government contracting issues with executive branch departments and agencies without litigation. She can be reached at astyles@akingump.com.