The Top 10 Compliance Challenges for 2020

A brief overview of the biggest compliance issues government contracting professionals likely will face this year (if they haven't already).

BY ERIC S. CRUSIUS, AMY L. FUENTES, KELSEY M. HAYES, AND VIJAYA S. SURAMPUDI

While government contracting can be extremely rewarding, it is not always for the faint of heart. Successful government contracting requires compliance with myriad requirements that can be found in agency-specific regulations, governmentwide regulations, statutes, class deviations, guidance, and more. Complicating matters further, sometimes these regulatory requirements are at odds with state and local requirements.

As we dive into the next decade of government contracts, some of the following compliance-related issues (presented in no particular order) promise to be some of the biggest challenges for government contracting professionals in 2020.

1. SBA Final Rule Implements the Small Business Runway Extension Act

In one of the biggest changes to the small business regulatory landscape in 2019, the long-awaited Small Business Runway Extension Act[1] became effective just after the new year on January 6, 2020, after the Small Business Administration (SBA) issued its final rule implementing the Act in December 2019.

There are three key elements of the Act and its implementing regulation that contractors should be aware of:

- First (and most important), the SBA's receipts-based size standard has now changed from a three-year averaging period to a five-year averaging period;
- Second, the final rule also includes a two-year transition period, during which time contractors can choose either a three-year averaging period or a five-year averaging period for calculating average annual receipts for size standards purposes during the transition; and
- Finally, the SBA clarified in the final rule that in a merger or acquisition transition, whether a seller or buyer must include the annual receipts and employees after the closing of the transaction depends on whether the transaction involved the sale of a segregable division or the sale of a separate legal entity.

Now that the Act is effective, contractors should be aware that:

- The SBA declined to make the final rule retroactive to the date of the Act (i.e., December 17, 2018). This means that the three-year averaging period continues to apply to offers submitted prior to January 6, 2020, because a company's size is determined as of the date the firm certified its size as part of its initial offer.
- Contractors may be able to keep (or reclaim in certain instances) small business size status for procurements during the transition period. This is dependent on whether using a three-year or five-year lookback period would be most advantageous to a company's size status.
- Contractors should consider adopting or revising internal policies regarding determination of size status so that the basis for the contractors' determination is well documented and communicated to relevant employees.
- Corporate restructuring may be a tool that small businesses wish to use in advance of an anticipated merger and acquisition transaction. By reorganizing a segregable division into a subsidiary prior to the transaction, a seller does not have to include the recently organized subsidiary's receipts and employees when computing its size post-closing.
- Contractors should cautiously contemplate how the five-year lookback period will affect their business, whether utilizing the three-year or five-year lookback period will be most advantageous during the transition period, and plan for how the Act may impact a company's small business status both now and in the future.

2. Interim *FAR* Rules Prohibit Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (a.k.a., the "Huawei Ban")

The Federal Acquisition Regulatory Council has issued two interim rules to implement Section 899 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019,[2] which generally prohibits government agencies, contractors, and grant or loan recipients from procuring or using "covered telecommunications equipment or services" produced or provided by certain Chinese companies as a "substantial or essential component of any system, or as criti-

cal technology as part of any system." Broadly speaking, the prohibitions in Section 899 will be implemented in two phases.

Phase 1

The prohibitions in Section 899(a)(1)(A) became effective on August 13, 2019. This Section prohibits agencies from "procuring or obtaining, extending, or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system" unless an exception applies or a waiver has been granted. These prohibitions were implemented with the creation of *Federal Acquisition Regulation* (*FAR*) Subpart 4.21 and the related solicitation provisions and contract clauses at FAR 52.204-24, 52.204-25, and 52.204-26, respectively.

The new annual representation requirement at FAR 52.204-26 mandates that an offeror must represent whether it *does* or *does not* "provide covered telecommunications equipment or services as part of its offered products or services to the government in the performance of any contract, subcontract, or other contractual instrument." If an offeror represents that it does not provide covered telecommunications equipment or services to the government, in response to FAR 52.204-26 or in the new paragraph (v) added to FAR 52.212-3, then it is not required to complete the representations in FAR 52.204-24, which is to be included in all solicitations and contracts. If the offeror represents that it does provide covered telecommunications equipment or services or has not made any representation in FAR 52.204-26 or FAR 52.212-3(v), it must still complete the representations required by FAR 52.204-24.

The clause at FAR 52.204-25 prohibits contractors from providing "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system" unless an exception can be applied, or the covered equipment or services are covered by a waiver. The clause imposes stringent reporting requirements that obligate the contractor to immediately notify the contracting officer when it discovers "covered telecommunications equipment or services *used* as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance[.]"[3]

In the event a contractor discovers covered equipment or services are used during contract performance, the contractor must report certain information *within one business day*. From there, within *10 business days*, the contractor must –

- Submit "any further available information about mitigation actions undertaken or recommended"; and
- Describe –
  - "[T]he efforts it undertook to prevent use or submission of a covered article,"
  - "[A]ny reasons that led to the use or submission of the covered article," and
  - "[A]ny additional efforts that will be incorporated to prevent future use or submission of covered articles."

Phase 2

Further prohibitions in Section 899(a)(1)(B) will become effective on August 13, 2020. These prohibitions restrict agencies from entering into contracts (or extending or renewing contracts) "with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This portion of the ban is far stricter than the interim rule effective in 2019.

Contractors must take steps to review their supply chains for the presence of any banned telecommunications equipment or services and ensure they are not incorporated into government deliverables. It is also worth taking steps to rid covered telecommunications equipment or services from the contractor's entire business operations to comply with the governmentwide ban that will go into effect later this year.

3. New *FAR* and *DFARS* Amendments Seek to Curb Agencies' Use of LPTA Source Selection Procedure

The Department of Defense (DOD) recently published a final rule[4] amending the *Defense Federal Acquisition Regulation Supplement* (*DFARS*) to implement limitations and prohibitions on the use of the lowest price technically acceptable (LPTA) source selection process and the FAR Council recently proposed a similar amendment to the *FAR*. As the contracting community is aware, LPTA is an evaluation method for selecting an awardee when the government expects to receive the

best value as the result of selecting the technically acceptable proposal with the lowest evaluated price. Agencies' use of LPTA has long been criticized for placing price or cost over technical value and is often seen as a "race to the bottom."

Under DOD's final rule, contracting officers may use the LPTA process only when certain criteria are met. The new rule also provides that contracting officers must avoid, "to the maximum extent practicable," using the LPTA process if a procurement is predominantly for the acquisition of:

- "Information technology services, cybersecurity services, systems engineering and technical assistance services, advanced electronic testing, or other knowledge-based professional services"[5];
- "Items designated by the requiring activity as personal protective equipment"[6]; or
- "Services designated by the requiring activity as knowledge-based training or logistics services in contingency operations or other operations outside the United States, including Afghanistan or Iraq."[7]

The proposed rule for civilian agencies includes the same limitations, but also includes "audit or audit readiness services, health care services and records, [and] telecommunications devices and services." If implemented, the proposed rule will amend FAR 15.101-2.

For many contractors, these rules are a step in the right direction – promoting technical merit over cost or price.

4. SBA Proposes the Consolidation of the Mentor-Protégé Programs

The end of 2019 saw a flurry of proposed and final small business regulatory changes. One of the most important proposed rules that contractors should be aware of is the SBA's proposed consolidation of the Mentor-Protégé (M-P) Programs.

Importantly, the proposed rule seeks to:

- Consolidate the M-P Programs by eliminating the 8(a) M-P Program and allowing any small business – including 8(a) concerns – to participate in the All Small M-P Program. If implemented, this proposed change will eliminate the requirement for the SBA to approve joint venture agreements between a mentor and 8(a) protégé.
- Consider whether to implement a size limitation on mentor eligibility following the SBA's receipt of suggestions that elimination of very large contractors from the pool of eligible mentors would benefit mid-sized contractors' ability to compete.
- Eliminate the three-contract limit for joint ventures between small businesses or parties to an approved M-P agreement for two years following receipt of its first award (which includes a novated contract).
- Require the recertification of a contractor's size status under unrestricted multiple award contracts (MACs) for:
  - Task order submissions of small business set-aside orders under an unrestricted MAC, and
  - Task order submissions for set-aside orders differing from

Agencies' use of LPTA has long been criticized for placing price or cost over technical value and is often seen as a 'race to the bottom.

the socioeconomic status of the underlying set-aside MAC.

- Authorize size protests relating to the new proposed recertification of a contractor's size status (as previously discussed).

Contractors should be aware that the proposed rule continues to be in the rulemaking process and should be on the lookout for the SBA's final rule expected later in 2020. Overall, the proposed consolidation of the M-P Programs is largely applauded by the industry as addressing the longstanding issues of inconsistency between the Programs because of the different approving entities, as well as proposing to eliminate the preapproval requirement of 8(a) joint ventures. This may prove difficult in practice due to unknown timing constraints that companies cannot rely on. Additionally, there is some concern over the feasibility of implementing the consolidated M-P Program due to limited resources from the agency. Only time will tell whether these changes can be effectively implemented.

5. New DOD Cybersecurity Standard: The Cybersecurity Maturity Model Certification (CMMC) Program

DOD's Office of Acquisition and Sustainment (OA&S) is launching the CMMC program to enhance the protection of controlled unclassified information (CUI and other nonpublic information) within the supply chain. Beginning in June 2020, some requests for information will require offerors to be certified at the appropriate CMMC level. Likewise, in September 2020, requests for proposals will require the same.

DOD recognizes that many security risks have arisen due to several high-profile breaches under the current acquisition system — where contractors provide individualized cybersecurity plans in accordance with the security controls in the NIST SP 800-71. However, these plans are generally provided post-award and depend on contractors' self-certification.

The CMMC program is expected to measure the maturity of a company's institutionalization of cybersecurity practices and processes. Through combining several cybersecurity control standards into a single unified standard for cybersecurity, the CMMC program intends to designate maturity levels ranging from "Basic Cybersecurity Hygiene" to "Advanced." The most basic level is "Level 1" and the most sophisticated level is "Level 5." Each level is designed to minimize the risk against a specific set of cyber threats relevant to that procurement by assigning the associated security controls and processes. Contracting officers will be required to assess which CMMC level is required for each procurement and to include that CMMC level in the solicitation. DOD advises that these levels will be modified on a yearly basis to ensure the cybersecurity controls remain current as cyber threats evolve.

Importantly, contractors must be certified by a third-party auditor who will evaluate a contractor's cybersecurity hygiene and certify (or not certify) a contractor at a desired level. DOD recently released the initial standards and the Accreditation Board is developing training for potential assessors who will be charged with assessing companies' compliance with the appropriate CMMC level they seek.

The CMMC program is expected to measure the maturity of a company's institutionalization of cybersecurity practices and processes.

There is no indication how long these certifications will be valid, but DOD has noted that –

- It is advising all companies against publishing their certifications publicly, such as on their company websites, to avoid these certifications becoming a check-the-box exercise for contracting officers; and
- Contracting officers will be allowed to request recertification under certain circumstances.

Importantly, there are no exceptions for small businesses, commercial products, or whether the contractor will ever possess CUI while performing the relevant contract. All contractors *and* subcontractors will be required to be certified at the appropriate CMMC level for *each and every* procurement. The only variable between procurements will be the CMMC level required.

DOD recognizes that this is a huge undertaking and contemplates it will take at least five years to fully implement. It has further noted that its goal is for CMMC to be cost-effective and affordable for small business. To that end, DOD has noted that the cost of the certification should not be prohibitive. Further, DOD is treating the cost of certification as allowable reimbursable costs.

The program is ripe to bring new enforcement mechanisms to cybersecurity and to build on the already growing number of False Claims Act (FCA)[8] actions involving cybersecurity standards. Whether a business has the proper CMMC level of certification is also likely be a hot issue in protests. Contractors should prioritize becoming familiar with these requirements and be prepared to tackle the upcoming certification process.

6. OFCCP Reports Record Recoveries in 2019

The Office of Federal Contract Compliance Programs (OFCCP) reported that in 2019 it hit the highest three-year period on record for recoveries against government contractors, recovering over $40 million in monetary settlements.

The basis for many of these allegations against government contractors has been a violation of Executive Order 11246, "Equal Employment Opportunity." Pursuant to the Executive Order, federal contractors with over $10,000 worth of business with the government in one year are prohibited from discriminating in employment decisions on the basis of race, color, religion, sex, sexual orientation, gender identity, or national origin. Contractors are also required to take affirmative action to ensure the company is providing equal opportunity in all aspects of employment.

OFCCP's increased recoveries should serve as a gentle reminder to contractors to review hiring and employment practices and to update affirmative action plans to ensure compliance.

7. Updated *FAR* Counterfeit Reporting Requirements

The FAR Council published a final rule, effective December 23, 2019, setting forth new counterfeit reporting requirements. The final rule institutionalizes a mechanism for *all* contractors – both civilian *and* defense contractors – to report the use of certain counterfeit and suspect counterfeit parts and certain major or critical nonconformance to the Government–Industry Data Exchange Program (GIDEP).

The new *FAR* provision[9] and clause[10] covers both civilian and defense contracts that are above the simplified acquisition threshold.[11] Covered contractors must provide written notice to their contracting officers, within 60 days of becoming aware or "having reason to suspect" that any part purchased for delivery to or purchased on behalf of the government is counterfeit or suspected to be counterfeit. The suspected counterfeit item must provide reasonable doubt of its authenticity through inspection, testing, record review, or notification from a third party. All suspected counterfeit items must be kept for review and disposition by the contracting officer. Further, the contractor must submit a report to GIDEP within 60 days of becoming aware or having a reason to suspect an item is counterfeit.

The final rule requires FAR 52.246-11, "Higher-Level Contract Quality Requirement," to be flowed down to all subcontracts without any alterations involving these items. There are four distinct contract types that will be impacted by this final rule:

- Items that are subject to higher-level quality standards, such as those where the nonconformance could lead to a higher risk of performance (e.g., complex and critical items);
- Items the contracting officer has determined are "critical," such as those likely to result in hazardous or unsafe conditions or for which failure would prevent performance of an agency's critical missions;
- Electronic parts or items containing electronic parts; and
- Services provided in conjunction with any of these items.

Ultimately, the rule has more bark than bite due to the limited require-

ments on contractors to monitor their supply chains and its limited applicability to certain contracts. The rule itself also does not require companies to implement any systems or mechanisms to detect and avoid counterfeit parts. Further, the rule provides "carve-outs" for certain contracts, such as commercial item contracts and certain medical devices. It also has limited application for contracts with –

- Foreign corporations with no offices, locations, or fiscal paying agents in the United States;
- Items that contractors know are subject to an ongoing criminal investigation; and
- Single source items (i.e., items that have not been sold to any other company).

The *FAR* provision and clause present another policy measure designed to address and attack risks within the supply chain. This focus on supply chain management suggests that compliance and risk management will likely be on the forefront of the government's enforcement radar and may lead to an increase in investigations.

8. Proposed Regulations Seek Expanded Scope of CFIUS Review

There has been a lot of change when it comes to foreign ownership or investment in companies that have contracts with the federal government. At the center of that is the Committee on Foreign Investment in the United States (CFIUS).

Following the passage of Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA),[12] the scope of investments or transactions that will be reviewed by CFIUS has expanded. This was detailed in proposed regulations released in fall of 2019. Highlights include:

- Nonpassive investments by foreigners will be reviewable under certain circumstances (broadly speaking, investments in companies that house critical technology, involve critical infrastructure, or have sensitive personal data of U.S. citizens);
- Certain real estate transactions will now be subject to review by CFIUS (though this review is highly dependent on the location of the real estate – e.g., if it is within one mile of a U.S. military installation); and
- Investments and transactions that allow a substantial interest by foreign governments.

Notably, the proposed regulations also contemplate a "white list" that would contain foreign investors (transactions are not included) that are exempt from CFIUS requirements. As the proposed regulations noted, such a list promises to be very short.

Contractors that may be subject to these new requirements should monitor the final regulations closely when they are released.

9. Cybersecurity *Qui Tam* Actions on the Rise

Cyberattacks have skyrocketed in recent years, leading to increased focus on preventing attacks and protecting sensitive information. In turn, this has led to increased enforcement efforts by the government concerning contractors' noncompliance with cybersecurity regulations.

As one example, a company recently settled a *qui tam* lawsuit with the New York Attorney General that alleged the company's software, which was designed to control security camera systems, had flaws that rendered the system vulnerable to hackers. The lawsuit alleged that the company was aware of these flaws and failed to disclose the flaws after selling the software to U.S. state governments and the federal government (including every branch of the U.S. military).

In another example, a California judge recently allowed a relator's cybersecurity FCA case to proceed, denying the company's motion to dismiss. The relator alleged that the company failed to comply with DFARS 252.204-7012, which imposes reporting requirements on defense contractors and requires specific controls to be in place to safeguard technical CUI from cybersecurity threats. Specifically, the relator contended that the company fraudulently entered into contracts with the federal government, despite knowing that it did not meet the cybersecurity compliance requirements of DFARS 252.204-7012 and a related NASA regulation. The U.S. District Court of the Eastern District of California agreed with the relator, finding that these false statements were material to the government's decision to award contracts and pay the company. Thus, it allowed the case to proceed. This is the first time a court has found an allegation of noncompliance with a cybersecurity standard to form the basis of FCA liability.

Expect enforcement actions concerning cybersecurity to increase. Contractors should diligently monitor and update their cybersecurity programs as new rules and regulations have been recently enacted and should diligently comply with any control standards and reporting requirements. Contractors must also ensure the appropriate controls and measures are in place to protect sensitive data, prevent attacks, and detect breaches.

10. Highlights from the 2020 NDAA

Each year's NDAA is always a great look into the future of government contracting. Often, NDAA provisions turn into regulatory requirements over the following one to two years. Understanding each NDAA's requirements and thinking about how these affect a contractor or contracting agency can allow all to prepare for changes that are due to come.

While a thorough analysis of the provisions of the 2020 NDAA[13] is beyond the scope of this article,[14] a few items stick out:

- *Section 254* – Addresses the United States' shortfall in developing 5G technology. It requires a plan to implement and harness 5G technology, including research and development and strengthening outreach to industry.
- *Section 845* – Requires a closer look at modernizing the acquisition process. The Section 809 Panel[15] released its final report nearly a year ago, which outlined detailed recommendations on how to modernize the U.S. acquisition process. While some of these recommendations have already been adopted, others have not, and this may be an effort to jump-start that process.
- *Section 886* – Requires a report from the Government Accountability Office detailing how many contractors, in the last five years, have been found to have willfully or repeatedly violated the Fair Labor Standards Act[16] or the Occupational Safety and Health Act.[17] Perhaps this is a prelude to introducing an updated version of Fair Pay and Safe Workplaces.[18] Because its implementing regulations were rescinded, Fair Pay and Safe Workplaces regulations cannot be reintroduced in identical form.
- *Section 873* – Would allow payments to small businesses to occur in as little as 15 days under certain circumstances. This is a valuable tool for small businesses because they often expend a tremendous amount of resources to start working on a contract – often with limited resources.
- *Section 827* – Requires the General Services Administration (GSA) to review the relative cost of the different models being considered for the new e-commerce portal. GSA must review the e-commerce, e-marketplace, and e-procurement methods.

Other provisions of interest will impact intellectual property, the SBIR/STTR programs, the acquisition workforce, and federal supply chains. In addition, there are other sections of the 2020 NDAA that cover some of the topics previously discussed in this article.

Conclusion

While compliance headaches abound for the remainder of 2020, compliance does not have to be a hassle – especially if you get ahead. Fortunately, there are a lot of free resources to help contractors, such as this magazine. **CM**

Eric S. Crusius
Partner, Holland & Knight LLP
eric.crusius@hklaw.com

Amy L. Fuentes
Associate, Holland & Knight LLP
amy.fuentes@hklaw.com

Kelsey M. Hayes
Associate, Holland & Knight LLP
kelsey.hayes@hklaw.com

Vijaya S. Surampudi
Associate, Holland & Knight LLP
vijaya.surampudi@hklaw.com

ENDNOTES

1 *Pub. L. 115-324.*
2 *Pub. L. 115-232.*
3 Emphasis added.
4 DFARS 215.101-2-70, "Limitations and Prohibitions" (i.e., on the LPTA source selection process).
5 DFARS 215.101-2-70(a)(2)(i).
6 *Ibid.*, at (ii) (except when 215.101-2-70(b)(1) applies).
7 *Ibid.*, at (iii).
8 31 USC 3729–3733.
9 FAR 46.317.
10 FAR 52.246-26.
11 $250,000 for most agencies as of January 2020 pursuant to class deviations.
12 Enacted as Section 1701 of the 2019 NDAA (*see* note 2).
13 *Pub. L.* 116-92.
14 Editor's Note: For an in-depth review of the acquisition-related provisions of the 2020 NDAA, see: Joe Martinez, Chris Fetzer, and Tyler Thomas; "2020 NDAA Highlights," *Contract Management* Magazine (February 2020): 38–43.
15 Editor's Note: Officially the "Advisory Panel on Streamlining and Codifying Acquisition Regulations," the Section 809 Panel was created pursuant to Section 809 of the 2016 NDAA (*Pub. L.* 114-92) and charged with analyzing the defense acquisition system and delivering recommendations for improvement. The Panel was sunset in July 2019, and its collected reports – including findings and recommendations – are available at https://discover.dtic.mil/section-809-panel/.
16 29 USC 203, *et seq.*
17 *Pub. L.* 91-596.
18 Editor's Note: A policy originally issued via Executive Order 13673, "Fair Pay and Safe Workplaces" (July 31, 2014), it was essentially revoked by the passage of *Pub. L.* 115-11 (signed March 28, 2017), which overturned the Executive Order's implementing regulations.