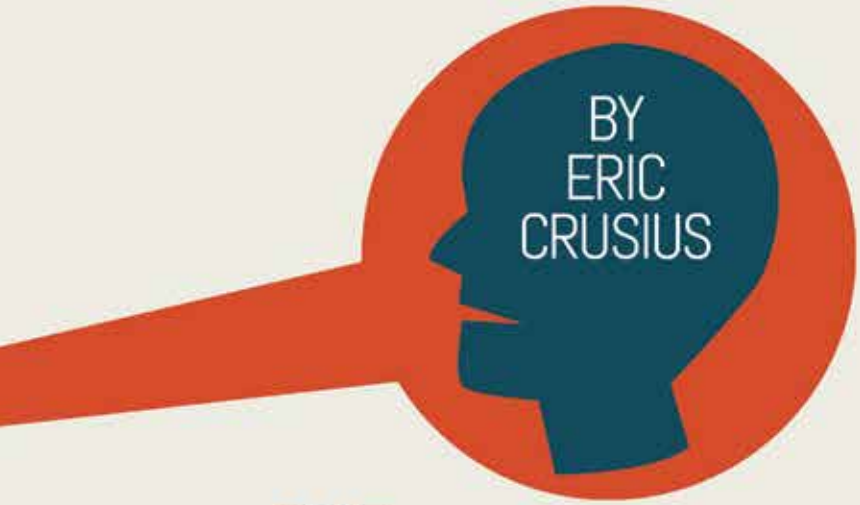
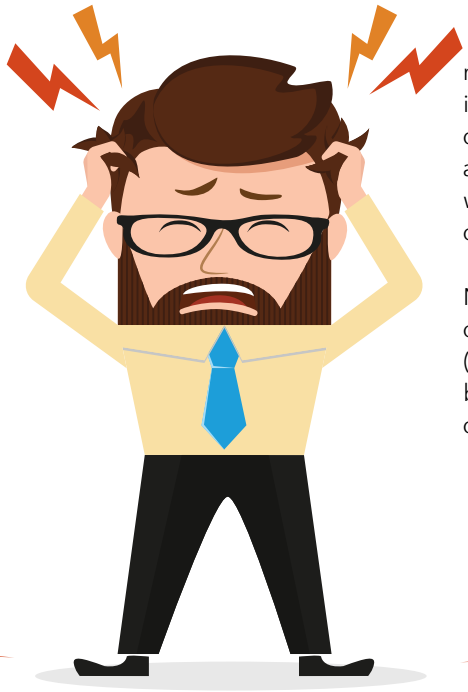


THE Top 10 Government Contracting Compliance HEADACHES IN 2017

Government contracting is not for the faint of heart.

This line of work requires compliance with thousands upon thousands of rules, regulations, statutes, case law, Executive Orders, agency issued guidance, and protests. Keeping your company in line and compliant with this "body of guidance" often requires frequent trips to the medicine cabinet to address compliance-induced "headaches."

With a change in administration and party, 2017 promises to offer additional complexities. Will the new president repeal many Obama-era Executive Orders and other instituted policy concerning acquisition? If he does, what will that mean for you? Will claims and disputes continue to grow—especially when the new president sees the price tags for complicated programs?



No matter what the year ahead brings, some of the following compliance-related issues (presented in no particular order) promise to be the biggest "headaches" for government contracting professionals.

1 Compliance with the Service Contract Labor Standards

No one really knows whether President Donald Trump's Department of Labor will act like a traditional Republican Department of Labor. In his early days in office, the new president met with labor leaders who were hopeful that he would not roll back a number of Obama-created worker protections and would continue with aggressive enforcement against contractors.

No matter what happens, however, certain labor protections are statutory and will continue to hang around (save for an act of Congress). One such statutory labor protection is the Service Contract Labor Standards statute (formerly known as the Service Contract Act).[1]

As the federal government continues to rely on contractors to perform an ever-expanding portfolio of services, more contractors are becoming subject to the Service Contract Labor Standards. The statute is applicable to contracts where the principal purpose is to provide services utilizing non-exempt service employees.[2] While the basic requirements of the statute are not complicated (minimum wages and benefits according to a wage determination), the "nooks and crannies" in the regulation often trip-up well-meaning contracting professionals and contractors.

Initially, it is up to the contracting agency to determine whether the statute applies. If it does, it is up to the contractor to:

Properly map employees;

Pay the wages set forth in an appropriate wage determination (or collective bargaining agreement); and

Provide hourly health and welfare, vacation, and holiday benefits.

Complications may arise when:

Determining employee anniversary dates,

Providing prorated benefits to temporary and part-time employees,

Figuring out the vacation entitlement, or

An agency does not include the appropriate statutory clause and wage determination on a contract that is clearly covered by the statute.

Contractors must also, among other things, notify employees as they are on-boarded of their Service Contract Labor Standards status, job title, and pay rate.

New Department of Defense (DOD) Source Selection Scheme

On April 1, 2016, DOD released new source selection procedures that covered the waterfront and are an essential read for every contracting professional.[3] The new procedures are notable for two things:

Decreasing the emphasis on the use of "lowest priced technically acceptable" (LPTA), and

Creation of new "value adjusted total evaluated price" (VATEP).

DECREASING EMPHASIS ON LPTA

DOD's new source selection scheme continues to deemphasize the LPTA source selection scheme—an initiative that has come under more and more criticism as it has been used for more and more sophisticated procurements. The main problem with LPTA is that it "handcuffs" the government into buying something because it is 1¢ cheaper than another option—even if the slightly more expensive proposal offers a much greater value.

I always likened this scenario to buying a vacuum cleaner. For many years, I purchased fairly cheap vacuum cleaners that would break down after about 18 months of use. I was finally fed up and purchased a more expensive and well-thought-of vacuum cleaner eight years ago, and it is still going strong. While my initial purchase price was higher, I have saved a lot of money, time, and aggravation over the last few years. LPTA does not allow a contracting professional the flexibility to purchase the more expensive vacuum cleaner in response to a bid.

LPTA also runs into trouble when what is "technically acceptable" is not precisely defined. Anecdotally, I have seen a number of protests lodged because of disputes over whether a contractor's proposal is technically acceptable, which slows down what should otherwise be relatively simple procurements.

INTRODUCING VATEP

DOD's new source selection scheme endorses the use of VATEP source selection evaluations. As described by DOD:

> In a tradeoff source selection, a total evaluated price is determined for each offeror. The source selection authority…must then determine if a higher-rated technical offer is "worth" the additional cost to the government. In VATEP, the "value" placed on better performance is identified and quantified in the [request for proposals]. This provides the offeror information to determine if the additional cost of offering better performance will put the offeror in a better position in the source selection. This also provides the [source selection team] the ability to assign a monetary value, or "monetize," the higher-rated technical attributes, thus taking some of the subjectivity out of the best value evaluation.[4]

This new source selection evaluation is different in that certain characteristics are essentially monetized. It will be interesting to see how agencies utilize this innovative option.

Cybersecurity Requirements

Cybersecurity is playing a more central role in every contracting professional's considerations before, during, and after the procurement process. In fact, President Trump has already focused on issuing a new cybersecurity Executive Order placing various cybersecurity related responsibilities with agencies.

WHERE DO CYBER THREATS COME FROM?

A good place to start every cybersecurity evaluation is to look at where the threats originate.[5] Most often, cyber intrusions and other threats originate from:

Criminal elements—use cyber-attacks for monetary benefits (such as selling personal information);

Other nations—use cyber espionage as a way to gain a geopolitical advantage; or

Insiders—perhaps the greatest threat to government agencies and contractors alike is the one posed by insiders (such as disgruntled organization employees that are motivated by animus or monetary gain).

Because insiders already have access to a critical computer system, less technical knowledge is required to create damage or a breach. There are also many instances where some insiders are inadvertent accomplices to cyber-attacks, such as clicking on links that they should not.

COMMON TYPES OF CYBER ATTACKS

Those looking to exploit systems use a variety of methods to reach their ends. These include:

"Denial of service" attacks–overwhelms a system and shuts it down;

"Phishing" and "spear phishing" attacks–often utilize realistic looking e-mails to entice recipients to click on links or download files that cause viruses which allow system infiltration; and

"War driving"–involves physically searching for and exploiting unsecured networks (sometimes by actually driving through neighborhoods).

THE PATCHWORK OF REQUIREMENTS

Cybersecurity requirements now come from a patchwork of statutory, regulatory, and various federal agency issued guidance, including:

Executive Order 13636,[6]

The Federal Information Security Management Act,[7]

Guidance promulgated by the National Institute of Standards and Technology (NIST),[8] and

Regulations promulgated by DOD that require notifications in the event of a breach and adherence to certain NIST recommendations.[9]

The foundation of NIST's cybersecurity effort is the cybersecurity framework it developed that helps organizations evaluate their cybersecurity risk and compare their current cybersecurity posture with their aspirational posture. NIST has also released special publications that have partially been incorporated into regulations. They include:

Special Publication 800-53–provides best practices in 14 distinct areas (called "families") of information security, including:

- Access control,
- Incident response,
- Physical protection, and
- Risk assessment; and

Special Publication 800-171–addresses "controlled unclassified information."

For contracting professionals, it is necessary to review the current state of cybersecurity regulatory requirements when drafting a procurement or responding to one. Contractors responding to bids that have new cybersecurity requirements may need to change how they manage their information technology prior to placing a bid.

Implied Certifications

Nearly one year ago, the Supreme Court (in *Escobar v. United Health Services*) held that certifications made by contractors can be implied.[10] In other words, so long as a requirement is "material" in the eyes of the federal government, a contractor does not necessarily have to explicitly certify compliance with that requirement in order for someone to bring a claim alleging a false claim.

It will be interesting to see how lower courts interpret what a "material fact" is in the years to come. Because each situation is so factually specific, there may not be a bright line rule, meaning contractors will need to institute more robust compliance systems to ensure they are aware of all potential implied certifications.

New Contractor Sick Leave Requirements

Over the course of his two terms in office, President Barack Obama signed a number of Executive Orders expanding rights of workers performing on government contracts. While many of these Executive Orders appear to be on the chopping block with the new administration, for the time being, they are required to be part of all applicable contracts–making compliance with these Executive Orders essential. Of particular note are the Executive Orders' sick leave requirements.

The sick leave requirements apply to certain services and construction contracts (as well as a few other minor categories of contracts) and mandate one hour of sick leave for every 30 hours worked. While sick leave does not have to be paid out to an employee upon termination, it must be reinstated if an employee returns within 12 months. Further, these requirements also apply to exempt employees and to workers spending at least 20 percent of their time on the government contract.

What makes these requirements especially headache-inducing is the fact that they are to be included *in addition* to other manda-

tory sick leave requirements established in localities and states around the country. Further, this is an additional requirement to the Service Contract Labor Standards[11] and Wage Rate Requirements (Construction)[12] regulations.

6 Budget Uncertainty

Over the last number of years, the federal government has lurched between funding crises (including a shutdown) and threats of hitting a debt ceiling. Even though the same party now controls the presidency as well as both houses of Congress, we should not underestimate the possibility that differences in funding priorities will create a possible funding disruption in the years ahead.

FUNDING CRISES

Should there be a shutdown, non-essential services will end because there is a lack of appropriations and the Antideficiency Act[13] prohibits work from continuing when there have not been appropriations. Contractors should prepare well in advance of a potential shutdown to determine how their contract is funded and whether the work performed is deemed "essential." Even if there are funding or essentiality exceptions in place, the work may not be able to be performed if the government facility is closed. While best practices anyway, contractors should have a handle on all of their contracts, how they are funded, and what would happen to the employees if there is a disruption of work.

DEBT CEILING

With respect to a debt ceiling, this occurs when money is appropriated, but the federal government does not have the money to pay for those services. Should the debt ceiling be hit, contractors would be obligated to continue working, but may not be paid for some time for that work.

The Fiscal Year 2017 National Defense Authorization Act (NDAA)

Typically, NDAA provisions do not usually impact government contracts immediately because regulations have to be promulgated to institute the change mandated by the NDAA provision. This year is no exception, though there are a few interesting provisions:

Section 803–within 180 days, DOD is required to issue a report regarding the modernization of the acquisition of services.

Section 807–includes the addition of performance goals and technical risk assessments for major defense acquisition programs.

Section 809–amendments relating to technical data rights.

Section 829–specifies that a preference for fixed-priced contracts and certain cost-type contracts would need to be approved by the service acquisition executive for the military department.

Section 831–reflects a preference for performance-based contract payments.

Section 835–task order protests are reinstated for DOD with a $25 million threshold.

Section 885–requires reports on bid protests within 270 days.

Section 886–requires a report by March 31, 2018, regarding the use of indefinite delivery/indefinite quantity contracts.

Section 887–requires a report on the use of flow-down provisions.

Section 888–requires justification for the use of brand-name requirements.

Right of First Refusal

Another Obama-era labor protection is the right of first refusal for existing employees on government contracts–known as the "Non-displacement of Qualified Workers" provision. This provision, instituted on January 18, 2013, requires incoming contractors to give a bona fide offer of employment to the incumbent non-exempt staff. There are exceptions to this requirement (such as poor performance by an incumbent employee or a change in staffing plan), but the burden is on the contractor to establish entitlement to an exception.

Bid Protests

While the statistics show bid protests to the Government Accountability Office (GAO) have been relatively "flat" in recent years, there is an increased awareness in the role protests have in the procurement process. Nearly half of the protests filed at GAO either result in the protest being sustained or an agency agreeing to take corrective action prior to the end of the protest. There is also now permanent authority to protest task orders so long as they are $10 million for civilian task orders and $25 million for DOD task orders.

Protests can often be avoided by effective communications between a contractor and the contracting agency.

Prime/Sub Disputes

"Frenemies" is a good way to describe the prime contractor/subcontractor relationship in many cases. Often, two different companies can act as a prime and sub on one contract, and compete against one another for work on another. Because of that, it is imperative for the prime/sub relationship to be memorialized in writing and not simply with the use of a purchase order.

STAY CURRENT

In addition, standard subcontract agreements used by companies should be continuously updated to reflect new *Federal Acquisition Regulation* (*FAR*), *Defense FAR Supplement* (*DFARS*), and other agency specific regulation requirements–as well as the requirements of a prime contract. Once a contract is entered into, the contracting staff should be made aware of the requirements to ensure they are followed *scrupulously*.

Conclusion

Unfortunately, we all know there are many more "headaches" on the horizon in 2017 than the 10 listed here. Some we know of and others will reveal themselves later in the year. However, paying attention to these top 10 headaches will ensure a real "migraine" does not occur when a potential problem arises. CM

ERIC S. CRUSIUS, JD

- Senior counsel, Holland & Knight LLP
- Represents government contractors in bid protests and other litigation matters before the Court of Federal Claims, GAO, boards of contract appeals, and other federal agencies
- Also represents corporations of all sizes in a variety of matters
- Lectures to industry groups, government agencies, and the American Bar Association
- Has appeared on NPR, Fox News, Government Matters, and Federal News Radio commenting on topics related to government purchasing
- President-elect, NOVA Chapter of NCMA

/in/ericcrusius

@EricCrusius

ENDNOTES

1. 41 USC 67.
2. *See ibid.*, at Section 2(a).
3. They can be found here: www.acq.osd.mil/dpap/policy/policyvault/USA004370-14-DPAP.pdf.
4. *Ibid.*
5. *See* GAO 15-758T.
6. "Improving Critical Infrastructure Cybersecurity" (February 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
7. 44 USC 3541, *et seq.* (enacted as Title III of *Pub. L.* 107-347, 116 Stat. 2899).
8. *See* https://www.nist.gov/cyberframework.
9. *See Defense Federal Acquisition Regulation Supplement* (*DFARS*) Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting"; *and* DFARS 252.204-7000-7015.
10. *See Universal Health Services, Inc. v. United States ex rel. Escobar* (No. 15-7, 2016 WL 3317565 (June 16, 2016)).
11. *See* note 1.
12. 40 USC 31, Subchapter IV (formerly known as the Davis-Bacon Act).
13. *Pub. L.* 97-258.