Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Top Gov't Contracts Policies Of 2019: Midyear Report

By **Daniel Wilson**

Law360 (July 22, 2019, 9:32 PM EDT) -- An increased focus on cybersecurity, major changes to important General Services Administration programs, new False Claims Act guidance and the always-important National Defense Authorization Act are just some of the important policy developments for government contractors so far this year.

Here are some of the key policy changes for government contractors that have come in the first half of 2019, alongside other changes set to come in the second half of the year.

The DOJ Provides Guidance on Cooperation in FCA Cases

In May, the U.S. Department of Justice rolled out its much-anticipated guidance on cooperation by entities facing False Claims Act litigation or investigations.

Among other provisions, the guidance document states that voluntary disclosure of false billing practices is the "most valuable form of cooperation" entities can provide, while also laying out 10 more forms of cooperation that could lead to leniency, as well as how any cooperation by defendants will be assessed.

Alongside a reduction in potential penalties and damages, cooperation credit could also come in forms such as public acknowledgement of assistance or a good word with regulators in charge of potential administrative penalties, the DOJ said.

The guidance is welcome in some ways, attorneys said, but they have also raised concerns about limits included in the guidance as well as what it fails to address.

For example, the guidance seems largely predicated on reaching a settlement, does not tie specific benefits to particular forms of cooperation, and notes that the DOJ will not grant credit for disclosures that are required by law, attorneys said. The DOJ also sets a ceiling on how much credit can be provided for cooperation, saying credit "may not exceed an amount that would result in the government receiving less than full compensation for the losses caused by the defendant's misconduct."

While the guidance seems "well-intentioned," actual damages plus costs is still a "pretty high floor" for liability, Wiley Rein LLP partner Roderick Thomas said. As an example he pointed to the use of contractual remedies instead of a damages settlement as appropriate in some circumstances.

"If a company's done a darn good job cooperating, and has darn good arguments on its liability, it seems to

me less than single damages should be on the table," he said. "In many matters, DOJ does yield on its views on single damages in negotiations, for a variety of reasons, and I'm hopeful that line attorneys do not misread this policy to prohibit that discretion."

Attorneys are hoping that the DOJ will come back with more comprehensive guidance, but regardless of the gaps in the initial guidance, "most sophisticated companies have started to amend, or will be amending, their internal compliance programs consistent with the new DOJ guidance," Bradley Arant Boult Cummings LLP partner Aron Beezley said.

The Government Continues to Ramp Up Its Focus on Cybersecurity

With the U.S. Department of Defense reporting that cyberattacks continue to grow in frequency and intensity every year, federal agencies — especially the DOD itself — have continued to put a strong emphasis on cybersecurity and on protecting classified and sensitive information.

Among related policy moves so far this year are a new draft of the National Institute of Standards and Technology Special Publication 800-171, issued in June, which covers protections for controlled unclassified federal information held by contractors and in other non-federal data systems, and underpins a lot of other federal cybersecurity standards.

That came shortly after the DOD announced its Cybersecurity Maturity Model Certification program, or CMMC. The DOD is planning to use third-party auditors to rate contractors on their ability to protect sensitive information on a five-point scale, and then work minimum rating requirements into defense contracts, it said. An initial framework for the program is expected to be released by January 2020, following a series of public and industry meetings throughout July and August.

The DOD also announced in a January memo that it would task the Defense Contract Management Agency with auditing contractors' compliance with regulatory requirements to protect "covered defense information," down through their supply chains. The House version of the pending fiscal year 2020 National Defense Authorization Act — further details of which are below — also pushes the DOD to create policies emphasizing supply chain security, including cybersecurity, as something that is not "a cost that defense contractors seek to minimize [but] a key consideration in the award of contracts."

That growing focus on cybersecurity has also spilled over beyond the policy arena into a first-of-its-kind ruling in May allowing a cybersecurity-based False Claims Act case in California federal court to move forward. Meanwhile, a U.S. Customs and Border Protection contractor, Perceptics, was suspended from bidding on new federal work in July after it was hacked and had photos of travelers and their license plates stolen — data CBP claimed shouldn't have been on its network at all.

The related compliance burden has been particularly tough on small businesses, as even meeting minimum requirements can be "very expensive for a small company," Mayer Brown LLP government practice chair Marcia Madsen said, suggesting that the government might want to find more appropriate standards, at least for small business set-aside contracts.

And commercial businesses who do most of their work outside federal contracting are also in a tough spot on cybersecurity regulations, Morgan Lewis & Bockius LLP partner Sheila Armstrong said.

"One area where my [commercial] clients are really struggling is trying to figure out, do they even have controlled unclassified information, and if they do, where is that information? Because, of course, the

requirements of the regulation is that you only have to protect a covered defense information system, so that could be limited in some circumstances, for example, to one particular server," Armstrong said.

Defense contractors, however, don't necessarily have to bear the full cost of meeting cybersecurity policy requirements. A DOD digital security official recently announced, as she rolled out more details of the CMMC program, that compliance with the security requirements would be an allowable cost, meaning defense contractors can claim reimbursement for related costs — although the details are still up in the air.

Other DOD Rules and the Section 809 Panel's Big Ideas for Changing Defense Acquisition

The DOD has also been busy in a number of other areas of policy that could affect contractors, including through the ongoing transfer of background checks for federal and industry security clearances to the department, expected to be completed by the start of October.

It also released a cloud strategy in February, its first "holistic view" of its ongoing efforts to move many of its information technology functions to online servers, followed in July by a digital modernization strategy intended to "[outline] how the department will increase agility and remain competitive within a constantly evolving digital global threat landscape," according to DOD Chief Information Officer Dana Deasy.

Among other pending and proposed acquisition policy changes, the DOD has also recently pleaded with Congress to streamline its software acquisition requirements, and is expected to roll out a final rule by the end of this year restricting the use of lowest-priced, technically-acceptable contracts, where bidders are assessed only on price, with no extra consideration given for meeting more than a minimum technical standard.

Contractors and lawmakers had both complained that the DOD had sometimes used the LPTA model inappropriately, for example for complex information technology acquisitions, and it was directed to restrict the use of the practice by Congress in the 2017 National Defense Authorization Act.

Also this year, a group of acquisition experts laid out a framework for many potential changes to DOD acquisition policy that may carry over into future National Defense Authorization Acts and DOD policies.

The Section 809 Panel, named after the section of the 2016 NDAA that mandated its formation, delivered the third and final volume of its report in January, a sprawling proposal with 98 suggested changes and improvements.

The overarching idea of the report is to move the DOD on from its often rigid acquisition system to a "dynamic marketplace" model that includes more communication between the department and industry and more use of streamlined acquisitions procedures and commercial and other "readily available" items — something the panel itself said was its "most revolutionary" recommendation — while in turn heavily restricting bid protests from losing bidders, among many other proposed changes.

The SBA Finally Puts Forward a Rule to Implement the Small Business Runway Act

After significant criticism from small businesses, their attorneys and lawmakers for dragging its feet, the U.S. Small Business Administration in June issued a much-anticipated proposed rule implementing the Small Business Runway Extension Act.

The bill, signed into law in December, is straightforward, allowing small businesses to use their average

revenue from the last five fiscal years to determine whether they qualify as a small business for federal assistance programs and set-aside contracts, replacing the current three-year revenue standard.

Its impact, however, will be significant, attorneys said, for example giving companies more time to adjust when facing the prospect of sizing out of small business standards, or better allowing them to stay eligible for small business programs despite after an outsized year.

"For small business, that is going to be helpful," Armstrong said. "Many of them will remain [legally] small for longer with a five-year average."

The SBA's failure to put the Runway Act immediately into effect has touched off strong debate, with the SBA itself arguing — repeatedly — that the law does not apply until it issues an implementing regulation. On the other side of the debate is the argument — based on U.S. Supreme Court precedent — that without a specified effective date, the law should have been treated as being in effect as soon as it was signed by the president.

"That created some confusion," Beezley said.

The SBA has still not yet indicated when it expects to issue a final rule, but its proposal is open for comment until Aug. 23. House lawmakers also recently passed legislation to give the SBA a hurry-up, requiring it to put a rule in place by the end of 2019.

The GSA Works to Consolidate Its Schedules and Roll Out Its Online Marketplace Pilot

The U.S. General Services Administration announced late last year that it will consolidate its 24 Federal Supply Schedules — also known as the Multiple Award Schedules — into one, then later announced that it will implement the change by October, the start of fiscal year 2020.

A series of broad, overarching contracts covering various categories of commonly used items and services such as security and janitorial services, office supplies, or information technology, the schedules are intended to give federal agencies a streamlined way to purchase things they frequently use without having to set up a new contract every time.

Even if the effect on specific vendors is small, the schedule consolidation is nonetheless likely to have a large cumulative impact, as the schedules are the most widely used acquisition vehicle across the federal government, with about $31 billion spent each year in total, according to the GSA.

And unlike some other pending regulatory changes, schedule consolidation is likely to be a win for both federal agencies and contractors, as although the schedules are already efficient in many ways, vendors need to have a contract for each schedule, and there are subtle differences between various schedules' requirements, creating unnecessary tracking burdens for contractors and paperwork burdens for both sides, attorneys said. Having a single schedule contract will mean a contractor only has one set of rules to abide by, among other benefits, they said.

"It will be helpful for schedule contractors who have multiple contracts to eventually have one point of contact," Armstrong said.

And in another big move for federal contracting, the GSA is also looking to shake up the way agencies purchase certain products by setting up a pilot for an "Amazon-like" e-marketplace portal, opening up

another streamlined way to purchase certain low-value commercial products, a market the GSA itself suggested in a July request for proposals could be worth about $6 billion a year.

This is just one of three models initially proposed by lawmakers as part of the 2018 NDAA, so the pilot process may take some time yet, with a number of key questions remaining to be answered, such as the new marketplace's impact on the schedules, attorneys said.

New Buy American Policies

President Donald Trump has made several moves to shore up Buy America and Buy American policies — intended to require the federal government to purchase American-made products and services whenever possible — since the start of his presidency, including two executive orders largely seen as preliminary or symbolic.

The first, issued in April 2017, ordered federal agencies to more closely monitor compliance with domestic sourcing requirements, and the second, issued in January this year, pointed to the importance of using domestic items in infrastructure projects.

In July, those vague orders were backed up by a far more prescriptive proposal, a new executive order raising the amount of U.S.-made components in a product to be considered American-made, from above 50% of the total cost to above 55%, with the potential to go even higher over time — and above 95% for any iron or steel used — while increasing a cost penalty applied to foreign-sourced goods during price comparison as part of the acquisition process.

These requirements, like with cybersecurity policy changes, will likely require federal contractors to look extensively up and down their supply chains to make sure they comply, attorneys claimed, suggesting that contractors keep a close eye on any implementing rule issued by the Federal Acquisition Regulatory Council over the coming months.

The Final 2020 NDAA

The National Defense Authorization Act, the sweeping annual defense policy and budget bill, is one of the few pieces of annual legislation that generally attracts broad bipartisan support, and it has become a catchall for changes to federal acquisition policy as a result of its must-pass nature.

The fiscal year 2020 versions of the NDAA don't include many high-profile acquisition changes, as had been typical in recent iterations of the bill, which is something many contractors will welcome, Madsen said. Each NDAA in the past three years had about 100 new provisions of acquisition law, she said.

"I'm sure it's upwards of 30 [provisions] involving commercial items [alone] — keeping track of all that, just from a regulatory perspective, is crazy," Madsen said.

Nonetheless, there are still a few proposed clauses that federal contractors should pay attention to in both the Senate and House versions of the legislation. One clause in the House bill, for example, touches upon the contentious issue of data rights, seeking to reinstate a repealed protection against the government using data rights while a contractor challenges the validity of the use restrictions on that data.

The House bill would also reduce the threshold for requiring enhanced post-award defense contract debriefings from $100 million to $50 million, with an amendment passed during floor debate also allowing

losing bidders on task orders worth up to $5.5 million and issued under an indefinite-delivery, indefinite-quantity contract, to seek an explanation of why they were not chosen.

And the bill would create a rapid acquisition pathway for certain software purchases and upgrades, as requested by the DOD, and would narrow the fee-shifting provisions for losing bid protests at the U.S. Government Accountability Office — which applies to large contractors with annual revenues of $250 million or more — by limiting the cost award only to direct costs incurred "in support of hearings to adjudicate covered protests."

Both chambers' versions of the NDAA would permanently authorize the DOD's mentor-protege program for small businesses, and the House bill would also create a formal dispute process for subcontractors to pursue prime contractors when they aren't paid, another provision that could be especially helpful for small businesses, attorneys said.

The Senate in June passed its $750 billion version of the bill in bipartisan fashion, and the House more recently passed its $733 billion version in an unusually party-line vote. The chambers will need to negotiate a final compromise bill.

--Additional reporting by Jeff Overley and Anne Cullen. Editing by Brian Baresch.