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 Policy Developments Of 2017

By **Daniel Wilson**

Law360, Nashville (December 20, 2017, 9:35 PM EST) -- 2017 introduced several major policy changes that will affect federal contractors' operations for years to come, from the implementation of a stringent new defense cybersecurity rule and the repeal of a deeply unpopular rule on labor violations to provisions of a sprawling Pentagon budget bill that may boost some contractors' business while imposing new requirements on others.

The Trump administration has made it clear that it is more intent on paring back regulations than adding to them, and at least one of those regulatory rollbacks will have a significant impact on federal contractors.

But a number of pending regulations that would affect federal contractors also made it through the year intact, perhaps none more important than a new cybersecurity requirement for defense contractors.

Congress was also busy, passing several provisions that were part of — or tucked into — the 2018 U.S. Department of Defense budget bill that could affect cyber, technology and commercial acquisitions, as well as the bid protest process and how unsuccessful defense contractors will be treated by the Pentagon.

Here are some of the most consequential policy moves for government contractors in 2017.

Repeal of Fair Pay and Safe Workplaces Rule

The Fair Pay and Safe Workplaces rule, introduced under the Obama administration and commonly referred to as the "blacklisting" rule by its opponents, was rolled back by Congress in March through a rarely used congressional review mechanism, with the enthusiastic support of the Trump administration.

The rule's main and most contentious clause would have required contractors and prospective contractors to list any recent violations of labor law in their contract bids, with "serious, repeated, willful or pervasive" labor law violations to be taken into account by contracting officers when determining whether to award or extend contracts — potentially serving as a de facto debarment from federal contracting, attorneys said.

It had drawn significant heat from contractors and their attorneys, who variously criticized the amount

of discretion and power it would have given contracting officers and the potential for interim, nonfinal decisions involving labor law to be used against companies; they also described the rule as a "solution in search of a problem," pointing to existing labor law enforcement mechanisms. The rule's repeal resulted in a collective sigh of relief among contractors.

New Cybersecurity Requirements for Defense Contractors

Defense contractors have until Dec. 31 to implement their compliance with Defense Federal Acquisition Regulation Supplement clause 252.204-7012, also known as the network penetration rule, driven by a marked increase in cyberattacks in recent years.

The rule, joined by a similar rule from the U.S. Department of Homeland Security, puts standards in place for how defense contractors should protect "controlled unclassified information" they have access to as part of their contracted work, and requires them to swiftly report any breaches into networks where it resides.

Contractors have called on the Pentagon to extend the compliance date, but the department has refused, and many companies, particularly smaller ones, are struggling with its implementation, if not directly then in meeting the requirement to "flow down" the rule throughout their supply chains, attorneys say.

"Companies are very worried that they're not going to be able to implement all of these somewhat arcane requirements in time," McCarter & English LLP government contracts practice co-lead Franklin Turner said. "The requirements are highly technical in nature, and they apply to essentially every DOD contract with the exception of commercial off-the-shelf items."

It's not just that implementing the rule on time is proving to be a struggle for many contractors; failure to meet the requirements of the rule opens them up not only to consequences directly from the DOD but also to new fronts of False Claims Act liability, attorneys noted.

"It's only a matter of time before we see a False Claims Act suit filed against a contractor for falsely certifying compliance with [that] DFARS clause," Bradley Arant Boult Cummings LLP partner Aron Beezley said.

The Growing Use of Other Transaction Authority

In a more positive move for defense contractors and potential ones, particularly those who are not traditional federal contractors, 2017 was a milestone year for the use of "other transaction" authority by the DOD, introduced on a permanent basis in the 2016 budget bill.

Other transaction authority, or OTA, streamlines much of the typical defense acquisition process in order to encourage commercial companies to contract with the DOD, and initial signals coming from its use have been positive, Dentons partner Jeniffer De Jesus Roberts said.

"From my experience, we have found that DOD has been very receptive to abiding by the more standard and traditional commercial contract terms, including provisions relating to limitation of liability, which historically has been a big [sticking point] for private industry wanting to do business with the government given the typical government position on limitation of liability provisions," she said. "So we have seen a big uptick in the use of OTAs and flexibility by DOD, and that's promising for a number of

our clients."

Demonstrating the growing use of OTA, the DOD announced in October that its Defense Innovation Unit Experimental, or DIUx — an office set up to draw commercial technology companies to work with the Pentagon — for the first time saw one of its pilot projects, contracted using OTA, grow into a full-blown contract when commercial cybersecurity firm Tanium won an up-to-$750 million, five-year contract from the Army.

"It's nice to see the program continuing and doubling down, if you look at their awards, and showing robust growth," Crowell & Moring LLP partner David Robbins said. "Especially in this budget environment, that a program like that continues and thrives is evidence of the importance of this emphasis on other transaction authority and intense focus on finding innovation, both to maintain technological superiority and to reduce costs."

Ellen Lord, undersecretary of defense for acquisition, technology and logistics, recently said that although the DOD is still struggling somewhat to get the word out to commercial companies, it is very interested in scaling up the model used by DIUx to help speed along acquisitions.

The 2018 National Defense Authorization Act

Given both the difficulty lawmakers often have in passing legislation, as well as the significant chunk of the federal discretionary budget that goes to defense, many of the legislative changes to federal contracting law that Congress makes are typically rolled into each year's National Defense Authorization Act, which sets out the budget and policy priorities for federal defense activities.

The fiscal year 2018 NDAA, signed into law in December, is no exception, making significant changes that will affect both defense and civilian contractors.

For example, in line with a perception among some lawmakers that a lot of frivolous bid protests are filed each year, wrongly holding up procurements — a perception both contractors and their attorneys have argued strongly against — the bill introduced a pilot program to require DOD contractors with annual revenues of $250 million or more to pay the government's costs in unsuccessful bid protests. That move has already proved unpopular, even before implementation.

"It goes against basic precepts of fairness — [that] you have the right to challenge an acquisition; that you have the right to challenge, as a company, whether or not your proposal was evaluated fairly ... and whether or not the government has gotten it right," Turner said. "And the idea that you would be penalized for asserting your rights is preposterous."

In return, the bill also introduces mandatory debriefing for defense procurements worth $100 million or more — or $10 million for small business and nontraditional deals — to the potential benefit of companies and the government alike, as long as the debriefings are more than rote, attorneys said, noting that one of the most common factors behind unsuccessful bidders protesting is a lack of information on why their bid was passed over.

"Contractors should be able to receive more information about the evaluation, and therefore be able to actually apply lessons learned," Beezley said. "And also it's quite likely that there will be a slight drop in protests because of these enhanced debriefing procedures — you'll probably see fewer protests that are filed by companies primarily because they did not get a sufficient debriefing and want to learn more

about what happened during the evaluation."

And in a clause that could shake up the way federal agencies acquire commercial items — a market the U.S. General Services Administration says is worth about $50 billion annually — the bill requires the GSA to establish "Amazon-like" marketplaces for commercial products, and gives the agency the green light to establish exemptions from typical procurement requirements to facilitate the new marketplaces, which could be crucial to business participation, attorneys said.

Also, the legislation directs the DOD to hire private audit companies to clear out a massive backlog in incurred-cost audits at the Defense Contract Audit Agency, letting DCAA focus on forward pricing audits. Attorneys said that backlog both is frustrating to existing contractors and discourages potential ones, and the authors of the bill say it is also a money-loser for the DCAA.

Finally, some less-publicized aspects of the bill could affect certain contractors, including changes to try to make transactions under the Foreign Military Sales program fit into a standard timeline, as well as a clause authorizing the commander of the Space and Missile Systems Center to create a "watch list" for poorly performing DOD space contractors, effectively excluding them from contracting until they get the blessing of the commander.

"I wonder if whoever requested this authority understands the amount of work they've signed the commander up for," Robbins said. "And just the due process requirements of this alone will be staggering; it's not going to fit into the usual [DOD vendor vetting exceptions]. And my other open question is, how on earth does that work with the existing suspension and debarment apparatus in the Air Force?"

--Editing by Brian Baresch and Breda Lund.