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 6 Gov't Contracts Policies To Watch: Midyear Report

By **Daniel Wilson**

Law360 (July 28, 2021, 10:41 PM EDT) -- The U.S. Department of Defense is expected to finalize a major overhaul of cybersecurity requirements for contractors in the second half of 2021, while contractors will also be keeping a close watch on proposed False Claims Act changes.

Here are six government enforcement priorities and pending policy moves that federal contractors should be watching during the rest of the year:

The Cybersecurity Maturity Model Certification Final Rule

Introduced as a response to what the DOD said was an ever-increasing level of "malicious cyber activity" against the defense industrial base, the department's Cybersecurity Maturity Model Certification program will require all defense contractors and subcontractors to have their cybersecurity programs assessed and rated.

Those ratings will run from Level 1 to Level 5, with a minimum level to be attached to certain DOD contracts over the next few years, and to all defense contracts by the end of fiscal year 2025, except for very low value and commercial-off-the-shelf item contracts, the department has said.

More than 200,000 companies will be impacted by the rule, with compliance costs expected to run to billions of dollars over the next few years, according to the DOD.

"Being able to present a certificate at the commensurate cybersecurity level will become a go/no-go threshold criteria to be eligible for award," said Crowell & Moring LLP partner Kate Growley. "So there are real dollars tied to this. That means that it is going to be a seismic shift in the way that government purchasers and contractors both approach cybersecurity."

The DOD in September 2020 released an interim rule to implement CMMC, and has said it expects a final rule to be released in September this year.

The interim rule drew more than 800 comments, with contractors and industry groups asking the DOD to be more flexible and take a more risk-based approach in its final rule, which is also expected to be a model for similar rules from other federal agencies, that would move away from a "one-size-fits-all" approach in the interim rule.

In a June hearing, small business representatives also made a plea for the department to better address

the circumstances of small businesses, saying the allegedly disproportionate cost burden placed on smaller companies to comply with CMMC could drive some out of defense contracting altogether.

Specific concerns raised by contractors have included whether there will ultimately be reciprocity between their existing Federal Risk and Authorization Management Program, or FedRAMP, certification and CMMC certification and how CMMC levels will map to existing cybersecurity requirements; the definitions regarding the types of controlled information they are supposed to protect; and the requirements that prime contractors will need to "flow down" to subcontractors, said Hogan Lovells senior associate Stacy Hadeka.

"Clarity on the reciprocity issue is really big, and hopefully they've taken on industry's comments with respect to providing some more insight and will at least address it in the background or introduction to the [final] rule, if not in actual [Federal Acquisition Regulation] provisions," she said.

Another key issue contractors want clarified is the process available to challenge their CMMC rating if the level they are given is not what they expected, said Venable LLP partner Dismas Locaria.

"If they don't get the certification that they need, they're going to be essentially foreclosed from certain work," he said, "And that's going to obviously impact their bottom line; they're going to need some due process. This is going to be the next area of significant litigation, because this is going to be life or death for some of these companies."

Finalization Of The 'Huawei Ban' For Contractors

The Federal Acquisition Regulatory Council — the DOD, NASA and General Services Administration — is also set to finalize a rule aimed at addressing potential national security threats within the federal supply chain, known as Section 889 Part B after the section of the 2019 National Defense Authorization Act that it stems from.

Section 889 formalized ongoing efforts, driven by fears of espionage, to keep technology made by Chinese suppliers perceived as having close links to the Chinese government and military out of the federal supply chain, most prominently telecommunications equipment giant Huawei Technologies Co. Ltd., giving rise to the clause's informal name: the "Huawei ban."

Section 889 Part (a)(1)(A) — or Part A — applies to federal government agencies, barring them from buying or using those products, and went into effect in 2019. Part (a)(1)(B) — Part B — applies to the use of those products by federal contractors and their suppliers, with an interim rule going into effect in August 2020.

Like with CMMC, the overall cost of complying with Part B has been estimated in the billions of dollars, and the interim rule has drawn heavy criticism from contractors and their attorneys over a lack of clarity around key terms in the rule, like the extent of the "reasonable inquiry" needed to look for banned equipment in a supply chain, or what "use" of a covered piece of equipment or service actually means.

While there have been some temporary waivers granted, the interim rule affords effectively no exceptions, applying broadly to equipment used by federal contractors and suppliers across all parts of their business, said Blank Rome LLP partner Merle DeLancey.

"Everybody's trying to tie 889 to some sort of nexus to a government contract," he said. "Sorry, Part B

doesn't require a nexus. You used it, period."

In addition to clarity regarding key definitions, other open questions that need to be addressed in the now-overdue final rule, originally expected around May, include how it will apply to personal equipment used by contractors' employees working from home, a much bigger issue since the start of the COVID-19 pandemic, DeLancey noted.

"They could be easy, or they could really turn things upside down," he said.

Senators' Proposed FCA Changes

Sen. Chuck Grassley, R-Iowa, introduced legislation earlier this week, alongside a bipartisan group of senators, intended to correct what he viewed as weakening of the False Claims Act stemming from lower courts' application of the U.S. Supreme Court's landmark 2016 Escobar decision.

Grassley, a key figure behind 1986 amendments to the False Claims Act that have spurred more whistleblowers to bring qui tam FCA suits on behalf of the government since, had been making noise about reining in what he had perceived as recent overuse of the U.S. Department of Justice's authority to ask for dismissal of whistleblower cases.

The bill would address that issue by requiring a hearing on such dismissal motions at which the whistleblower can weigh in, and other Grassley bugbears, including what the senator said was "confusion and misinterpretation" of the Escobar decision that had "made it all too easy for fraudsters to argue that their obvious fraud was not material [to a claim for payment] simply because the government continued payment."

It would also explicitly bar post-employment retaliation against FCA whistleblowers, and put parties involved in FCA cases on the hook for reimbursing the costs of the government for "fishing expeditions" during discovery that are considered overly burdensome or irrelevant to a case.

But much of the intent of the bill as expressed in lawmakers' statements isn't necessarily reflected in its actual language, attorneys recently told Law360, and they will be watching to see whether the bill changes as it goes to committee and perhaps eventually to the Senate floor.

How Will The GSA Proceed With Transactional Data Reporting?

The General Services Administration introduced its Transactional Data Reporting, or TDR, rule in 2016, seeking to move away from the model used for its massive multiple award schedule, or federal supply schedule, program where contractors have to report their commercial pricing to the government, to one where they would instead report their pricing based on sales to federal agencies.

The agency said the rule was the largest change to the MAS in more than two decades and touted it as a win-win for both agencies and contractors, increasing price competition and uniformity while easing reporting requirements on vendors.

Contractors and attorneys were immediately skeptical, arguing that it was simply replacing one set of reporting requirements with another, and the GSA subsequently attempted to respond to industry concerns, including making TDR optional rather than mandatory.

But it has continued to push forward with its TDR pilot, announcing in April that it would expand the pilot program after several years of what it deemed to be positive results, even amid a highly critical GSA Office of Inspector General report.

The watchdog argued that TDR "has yet to accomplish its intended purpose of improving taxpayer value," with related data "not being used to make decisions that affect pricing." It cited a "myriad" of reasons, including inaccurate and unreliable TDR data and lack of "basic understanding" among many contracting personnel regarding how to use the data.

Agencies including the GSA often adhere to the advice of their inspectors general, but the GSA seemed unfazed by the OIG's report, saying in a response to the report that it disagreed with many of the watchdog's conclusions and rejecting a recommendation that it end the TDR pilot.

"I think that the [GSA Federal Acquisition Service] commissioner is trying to balance a number of different approaches and cost benefits under both TDR and a traditional GSA Schedule model, which imposes significant compliance obligations on contractors … trying to identify an approach and perhaps make enhancements to the TDR pilot by giving better data access, more granular information to government buyers, rather than exiting the program entirely," said Crowell & Moring LLP government contracts group co-chair Peter Eyre. "But it's obviously something that we're going to be watching to see how that tension plays out."

What's Next For The DOJ's Procurement Collusion Strike Force?

Launched in late 2019 as a collaboration between the DOJ's Antitrust Division, U.S. attorneys' offices, FBI and several inspectors general to bring "coordinated national response" to antitrust and related issues in public procurement, the department's Procurement Collusion Strike Force spent most of 2020 building capacity and partnerships and training thousands of government personnel on how to spot collusion risks in public procurement.

But late in the year it began to put its plans into action, with the DOJ announcing in October the first indictment specifically stemming from the strike force, alleging an engineering company and its former executive were part of a decadelong conspiracy to rig bids for contracts with the North Carolina Department of Transportation.

That was followed in June this year by the first international case to be resolved by the strike force, involving an alleged bid-rigging conspiracy between Belgian security companies, which had affected the DOD and NATO contracts partially funded by the U.S., the DOJ said.

The strike force has brought a level and type of scrutiny to potential collusion in federal contracting that has not been seen before, including the use of data analytics to detect potential "suspicious bid patterns."

"This is a big deal because it is driving resources, and training, and focus into all of these areas," said Jenner & Block LLP government contracts practice co-chair David Robbins. "And more importantly, on the ground what I'm seeing is cases that are picking up DOJ attention at dollar values that wouldn't normally have done so. It's getting a lot more investigative resources; the priority of the government has been articulated. The full might of the government's procurement fraud apparatus is deciding 'we are sending strong messages.'"

More PCSF cases are likely to emerge later in 2021 and in 2022, with the DOJ having said in March that there were roughly 30 related grand jury indictments and investigations under way at that time linked to the strike force, ranging from local public works projects to larger defense and national security matters.

"I think it's an area ripe for enforcement and I think we'll see a lot more on the horizon here under the new administration," Venable's Locaria said. "There's no question that some contractors are too cozy with small businesses."

And the DOJ is not the only agency to step up efforts to rein in procurement fraud, Robbins said, pointing to an early July announcement of a new joint memorandum of understanding between U.S. Air Force law enforcement, investigative and procurement offices to form an "Acquisition Integrity Working Group" and collaborate on fighting acquisition fraud.

That effectively revives a program instituted roughly a decade ago, when the Air Force — which spends more than $70 billion on acquisition each year — had aggressively gone after fraud and suspended or debarred hundreds of bad actors, according to Robbins, who had previously led the Air Force's Procurement Fraud Remedies Office.

The MOU is another potentially big deal, "especially since the Air Force was a former leader [in fighting procurement fraud], and had been dormant for a number of years," Robbins said.

Acquisition Changes In The 2022 NDAA

The National Defense Authorization Act, the annual defense policy and budget bill, is one of the few pieces of legislation that routinely receives bipartisan support in Congress, and given its "must-pass" nature and the DOD's significant role in federal contractual spending, it often serves as a catch-all for federal acquisition policy changes.

The process for the fiscal year 2022 NDAA has kicked off later than usual for Congress after the White House was tardy in providing its budget request, and a final bill isn't expected until later in the year, likely past the beginning of the new fiscal year in October.

But the Senate Armed Services Committee marked up its version of the bill last week, and House Armed Services subcommittees are marking up their parts of the bill this week, ahead of the full committee considering the bill in September. There are many acquisition-related suggestions in the draft bills.

These include, for example, the Senate suggesting that the DOD assess its supply chain standards for microelectronics while requiring defense contractors to disclose the sources of printed circuit boards they use in certain acquisitions, and establish a working group to review and suggest how to update cybersecurity requirements in DOD weapons acquisition policy and guidance.

The Senate bill would also fund an Acquisition Innovation Research Center "to develop new and innovative acquisition policies and practices" and repeal a preference for fixed-price contracts, and includes several clauses aimed at making it easier and quicker for the DOD to purchase innovative commercial technologies, an issue it has long struggled with.