Defense Contracting Law Developments From 2019

By Joseph R. Berger

Law360 (January 10, 2020) -- The U.S. Department of Defense was at the center of many key developments in the government contracting legal field in 2019. Many of these events were driven by Congress, the annual National Defense Authorization Act, and the renewed great power competition that has shifted congressional and DOD priorities over the past decade, resulting in increased attention to technology innovation, acquisition reforms, the industrial base and supply chain security.

The DOD's attention to emerging technologies and prioritization of cybersecurity have continued to increase in recent years as challenges to U.S. technological superiority have grown. This year, as new security threats emerge, government contracting will remain key to the ability of the U.S. government to compete in the global technology race of the next decade.

Here are 10 developments from 2019 in the DOD contracting legal field to keep watch on in 2020, relating to the NDAA, cybersecurity, acquisition policy, other transactions, artificial intelligence, great power competition, total spending, robust enforcement, bid protests and the increased threat environment at home and abroad:

1. The National Defense Authorization Act for Fiscal Year 2020

The NDAA for FY 2020 was finalized when the House and Senate passed the conference report[1] and the president signed it into law on Dec. 20, 2019. A bipartisan summary of the NDAA for FY 2020[2] was released by the congressional committees with the conference report on Dec. 9, 2019. The NDAA's national defense top-line funding is $738 billion, with another $5.3 billion allocated for emergency disaster recovery. Among the many notable implications and developments in the DOD contracting field are:

U.S. Space Force

The creation of the U.S. Space Force will lead to new priorities and procedures in this area of DOD contracting, and the success of the space force mission will depend heavily on its contractor partners.

The NDAA establishes the U.S. Space Force as the sixth armed service of the United States, under the U.S. Air Force, and recognizes space as a warfighting domain, as stated in the conference summary. The NDAA creates a chief of space operations for the U.S. Space Force who will report directly to the secretary of the Air Force.

In addition, a Senate-confirmed assistant secretary of the Air Force for space acquisition and integration will serve as the "senior space architect" who will lead the acquisition of space systems as

the chair of the Space Force acquisition council, and take on service acquisition executive responsibilities for space systems and programs as of 2022.[3]

Cyber Operations and Cybersecurity

The annual NDAA, as it has for several years, enhances the DOD's cybersecurity strategy and cyberwarfare capabilities, and strengthens cyber operations and congressional oversight. The NDAA for FY 2020, among numerous other cyber measures:

- Establishes Principal Cyber Advisors on military cyber force matters for each military service;
- Directs an annual report on military cyberspace operations; and
- Directs a zero-based review of DOD cyber and information technology personnel.[4]

Section 1648 of the NDAA also endorses the current DOD plans for the Cybersecurity Maturity Model Certification, or CMMC, program. Section 1648 requires the secretary of defense to develop a comprehensive framework to enhance the cybersecurity of the U.S. defense industrial base no later than Feb. 1. This will include "the responsibilities of the prime contractors, and all subcontractors in the supply chain, for implementing the required cybersecurity standards, regulations, metrics, ratings, third-party certifications, and requirements identified."

Pentagon Acquisition Workforce Reforms

Among the NDAA's acquisition reforms are workforce reforms. Accordingly, the NDAA requires the DOD "to redesign the Acquisition Workforce certification, education, and career fields by leveraging nationally and internationally recognized standards," which will rely on third-party accreditation programs that may permit closer harmonization with the private sector.

In addition, the NDAA establishes a defense civilian training corps to train civilians for public service in the DOD and to address "critical skill gaps in the DOD's civilian workforce." The NDAA also requires the DOD to establish extramural research activities focused on innovative acquisition processes, leverage expertise outside of the DOD, and provide policy alternatives to DOD and Congress.[5]

Emerging Technologies

The NDAA "directs policies to ensure that the national security innovation base is poised to meet long-range emerging threats and the rise of global competitors," as highlighted in the conference summary.

Accordingly, the NDAA includes a host of measures supporting the development of emerging technologies including cyber science and technologies, artificial intelligence, hypersonic capabilities, quantum information science, and emerging biotechnologies.

The NDAA also "recognizes the importance and urgency of establishing a Departmentwide 5th Generation (5G) [telecommunications] strategy to

enhance military capabilities." The NDAA also establishes new pathways "for the most promising small businesses to commercialize their innovations for the DOD market."[6]

The Defense Industrial Base and Supply Chain

The NDAA also "continues the work of previous NDAAs to enable the DOD to assess and mitigate risks to its supply chain posed by advanced intelligence services ... that seek to exploit vulnerabilities to erode our military advantage."[7]

NDAA Title VIII, Subtitle E relates to industrial base matters, and includes a large number of provisions reflecting congressional and DOD concern over the vitality, health and security of the defense industrial base, as well as the defense supply chain.

For example, Section 845, "Modernization of Acquisition Processes to Ensure Integrity of Industrial Base," requires the DOD to digitize and streamline its existing approach to identifying and mitigating risks to the defense industrial base, including supply chain risks, as well as risks posed by violations of law by contractors. The analytical framework must also include assessment of the DOD acquisition processes and monitoring of the health and activities of the defense industrial base. The conference report also noted the importance of contracting as the foundation of the DOD's relationship with the industrial base.

The NDAA and conference report reflect continuing congressional concern over vulnerabilities in the DOD supply chain, and continuing efforts to improve the security and strength of the defense industrial base. These concerns were also reflected in numerous regulatory actions taken in 2019 by DOD, additional agencies and the Federal Acquisition Regulatory Council, addressing various security risks in the defense supply chain, including foreign sources of equipment and counterfeit parts. These concerns have also been reflected in DOD's new CMMC program.

2. DOD Plans for Cybersecurity Certifications

The DOD is preparing to implement its CMMC program for contractors in 2020, which will ultimately require third-party certifications for more than 300,000 companies in the DOD supply chain. The DOD published the preliminary versions of the draft CMMC model framework last year and is expected to release Version 1.0 this month.

The CMMC enforcement mechanism will build upon, and significantly add to, the current DOD cybersecurity regulations and the incorporated requirements developed by the National Institute of Standards and Technology, or NIST. As noted above, the CMMC program was endorsed in the NDAA for FY 2020.

The Office of the Undersecretary of Defense for Acquisition & Sustainment, or OUSD(A&S), worked throughout 2019 with DOD stakeholders to establish the requirements for the CMMC.[8] OUSD(A&S) has explained that solicitation proposal instructions and evaluation criteria will set the required CMMC level for specific contracts at levels one through five.

Related cybersecurity developments within the last year also included a notable False Claims Act district court decision and a significant FCA

settlement, suspension and debarment news, and other enforcement actions relating to cybersecurity.

These events, as well as continuing news throughout the year of cyber breaches and cyber advances, and threats by competitor nations and governments, serve as a reminder that while the DOD implements the new certification mechanisms, contractors must devote substantial resources toward compliance with both the new standards and the current cybersecurity regulations, including the comprehensive Defense Federal Acquisition Regulation Supplement and NIST requirements.

3. DOD Embracing Acquisition-Policy Reforms

The DOD has been preparing and is in the final stages of a major rewrite of its official acquisition guidance — the DOD 5000 series directives and instructions — and the formal rollout of the Adaptive Acquisition Framework, or AAF, a redesign of the defense acquisition system that the DOD has described in writings and speeches as the most transformational change to acquisition policy in decades. The DOD acquisition guidance rewrite and implementation of the AAF will have a major impact on acquisition reform in 2020.

The latest developments can be found on the website of the DOD's new Office of Acquisition Enablers,[9] as well as the website of the Defense Acquisition University.[10] The AAF will provide six separate acquisition pathways and will be accompanied by new courses at the DAU.

The six pathways will embrace the DOD's intent to simplify acquisition policy, employ tailored acquisition approaches, conduct data-driven analysis, actively manage risk and emphasize life cycle sustainment.

Undersecretary of Defense for Acquisition and Sustainment Ellen Lord gave a press briefing on Dec. 10, 2019, in which she discussed the past year's acquisition reform efforts and previewed goals for 2020.

She began by recognizing the DOD's 175,000 acquisition professionals and the goals of acquisition policy in support of the DOD's global mission. Lord discussed the rewrite of DOD guidance and the forthcoming AAF, expected to be published this month, and their importance to the DOD's acquisition reforms.

Lord also noted the DOD's delegation of major defense acquisition programs to the services, a 15% reduction in the number of DFARS clauses from 352 to 298 and a reduction in procurement administrative lead time.

Lord highlighted the DOD's success with other transactions; the DOD's plans for the CMMC; the development of the middle-tier acquisition policy, which enables program managers to field mature technology within five years; and the newly established intellectual property cadre of DOD professionals to coordinate intellectual property policy and address concerns over the impact of cybersecurity threats on IP rights.

She said she is also "committed to providing our workforce new insights and best practices that we can take from the commercial sector," and previewed priorities for 2020:

> In 2019, there was an enormous amount of focus on acquisition. In 2020, we will keep that momentum going, focusing on the CMMC rollout, 5G, protecting intellectual property, fielding counter-[drone] systems and strengthening the national technology and industrial base.

4. DOD Other Transactions Continue to Increase

Other transactions, or OTs, saw another year of significantly increasing DOD use for research, prototypes and production in 2019. Authorities for OTs allow the DOD to negotiate agreements faster, without the delays of most bid protests and without requiring companies or the DOD to follow traditional procurement regulations, including the FAR.

The U.S. Government Accountability Office released a report in November 2019 concerning the DOD's use of OTs for prototype projects, reporting that total obligations on OTs for prototypes increased from $1.4 billion in FY 2016 to $3.7 billion in FY 2018.

According to the report, the DOD is encouraging the use of OTs as a way to acquire innovative and emerging technologies, including in the areas of cyber, space, artificial intelligence and drones. According to other reporting, DOD spending on all types of OTs in FY 2019 may have reached $7 billion or more.

It remains to be seen how high spending on OTs could go in future years, and how well the use of OTs will help the DOD compete in the defense technology race. In addition, it remains to be seen how well OTs will improve the procurement process for the DOD without the accountability and transparency of standard bid protests at the U.S. Government Accountability Office and the U.S. Court of Federal Claims.

In Space Exploration Technologies Corp. v. United States,[11] a major OT procurement by the Air Force for space launch services was protested at the COFC, which found it lacked jurisdiction, but granted a venue transfer to a U.S. district court. To the extent that the U.S. district courts provide an alternative protest venue, the DOD will need to adapt to this new forum for review of its OT awards.

5. Artificial Intelligence Impacts DOD and National Security

In 2019, the U.S. government continued to support the development of artificial intelligence technologies with defense and national security implications, with actions including the February 2019 executive order on AI and the release of the DOD's 2018 AI strategy.[12]

The National Security Commission on Artificial Intelligence, which was established by the NDAA for FY 2019, released its interim report on Nov. 4, 2019.[13] The report identifies five lines of effort necessary to preserve U.S. advantages: investment in AI research and development; application of AI to national security missions; training and recruitment of AI talent; protection of U.S. technology advances; and global AI cooperation.

With respect to investment in AI, the commission found that federal research and development

funding for AI "has not kept pace with the revolutionary potential it holds or with aggressive investments by competitors. Investments that are multiple times greater than current levels are needed."

The modern technology race had its origins with the Russian launch of Sputnik, which led to the creation of NASA and the Apollo missions, as well as the first other transaction authority. According to the National Security Commission on Artificial Intelligence, however, within this frame of reference, the United States is now moving backward in terms of R&D funding for new technology:

> The U.S. Government knows how to infuse resources into audacious technology projects, as it did for the Apollo space program or the Human Genome Project. While the Chinese government has made ambitious public commitments to technology megaprojects, the United States has returned to pre-Sputnik levels of federal R&D funding as a percentage of [gross domestic product]. Indeed, the trend is going in the wrong direction.

In addition to the commission's report, at the end of October the Defense Innovation Board released a proposed set of guidelines on the ethical use of AI by the DOD. **Law360 reported** that the new ethics principles may make it easier for commercial AI firms to work with the DOD.[14]

In November 2019, the Congressional Research Service also released an updated report on AI and national security, asking how Congress might influence defense acquisition reform initiatives that would facilitate AI development.[15] AI research is underway in the fields of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and in a variety of autonomous vehicles or drones, according to the CRS report.

But AI also presents unique challenges for the military, "particularly because the bulk of AI development is happening in the commercial sector,"[16] and the "defense acquisition process may need to be adapted for acquiring emerging technologies like AI."[17] In addition, international rivals are "creating pressure for the United States to compete for innovative military AI applications."[18]

The CRS report notes China's announcement in 2017 of its plan to take the lead in AI by 2030, and Russia's similar announcement a few months later that it would pursue global leadership in AI technologies. But AI is just one example of how U.S. procurement priorities have been influenced by so-called great power competition.

6. Great Power Competition Shifts Priorities

The technology race between the United States and other nations continues to impact DOD procurement processes and priorities, as it has throughout the past decade. The CRS released an updated report, "Renewed Great Power Competition: Implications for Defense — Issues for Congress," in December 2019.[19]

According to the CRS, the shift to renewed great power competition was acknowledged by formal defense strategies under both the Obama and Trump administrations, which reoriented U.S.

national security strategy and defense strategy toward an "explicit primary focus on great power competition with China and Russia."

This shift has had major implications for defense funding, strategy, plans and programs, which in turn have affected DOD contracting priorities. The procurement-related issues affected, according to the CRS, include maintaining U.S. technological superiority; innovation and speed for weapon system development and deployment; and supply chain security (among many other strategic issues). In addition, new "operational concepts" require increased integration across the "multiple domains of land, air, sea, space, electromagnetic, information, and cyberspace." According to the report:

> In response, DOD has taken a number of actions in recent years that are intended to help maintain U.S. military superiority over improving military capabilities of other countries, including funding for developing new militarily applicable technologies such as [AI], autonomous weapons, hypersonic weapons, directed-energy weapons, biotechnology, and quantum technology, as well as actions intended to shorten acquisition timelines, meaning the time needed to develop and procure new weapons and equipment.

And as a result, DOD officials have argued that U.S. defense acquisition policy should be adjusted "to place a greater emphasis on innovation and speed of development and deployment as measures of merit in defense acquisition policy (alongside more traditional measures of merit such as minimizing cost growth, schedule delays, and problems in testing)."

Accordingly, the military services in recent years have taken actions to move toward more rapid acquisition of new capabilities, including the use of new authorities for OTs and middle tier acquisition, as noted by the CRS. These DOD and congressional priorities, and pressure for rapid acquisition of new technologies, can be expected to continue in future years and throughout the next decade.

7. Total Spending Near Historic Highs

According to a GAO report updated in May 2019, the U.S. government spent more than $550 billion on government contracting in FY 2018, an increase of more than $100 billion from FY 2015, which was "largely driven by spending on national defense."[20]

According to the GAO, of the $554 billion in total contract spending, $358.3 billion was attributable to the DOD, while $195.8 billion was by civilian federal agencies. Small businesses received $72.2 billion in DOD prime contracts and $52 billion in civilian contract awards.

According to some news reports last year, the total government contracting spend may have reached an even higher level in FY 2019, near $560 billion and possibly surpassing the record high level reached in FY 2010. According to data from the OMB, IT spending is a significant component of overall spending, with federal IT spending planned to be about $88 billion in FY 2019 and the same in FY 2020, including about $51 billion for civilian agencies and $37 billion for the DOD (excluding

billions more in classified spending). According to reporting in 2019 by The Washington Post, total U.S. military spending may also reach near-historic highs in 2020.

Separately, U.S. foreign military sales supervised by the DOD's Defense Security Cooperation Agency were above $55 billion for FY 2019 and FY 2018, reflecting higher levels than recent years and increased spending by foreign governments. Direct commercial sales to foreign end-users, supervised by the U.S. Department of State, accounted for an additional $136 billion in FY 2018 (and likely a similar amount last year).

While the high numbers in U.S. spending on government contracts as well as foreign spending may create opportunities for businesses of all sizes, this may also bring high levels of bid protests, contractual disputes and enforcement actions.

8. Enforcement Remains Robust

In November 2019, the U.S. Department of Justice and U.S. attorneys offices, along with the DOD, the Federal Bureau of Investigation and the U.S. Postal Service, announced the creation of the Procurement Collusion Strike Force, which will step up the government's enforcement efforts targeting bid rigging and antitrust violations in government contracting, grants and program funding.

The DOJ also announced major FCA settlements involving the DOD throughout the year, including cases relating to bid rigging, labor charges, subcontracting, small-business eligibility and defective products.

The DOD's own continuous enforcement efforts also remain robust, including audits, and administrative and criminal investigations, as reflected in the DOD Office of Inspector General semiannual reports to congress.[21]

According to the most recent DOD OIG semiannual report for the six-month period ending Sept. 30, 2019 (released on Dec. 2), investigations by the Defense Criminal Investigative Service, or DCIS, resulted in $537.1 million in civil judgments and settlements and $181.3 million in criminal fines (in addition to $885.3 million and $72.7 million respectively for the prior six- month period).

As of Sept. 30, 2019, DCIS had 1,646 ongoing investigations. These cases related to criminal allegations of procurement fraud, public corruption, product substitution, health care fraud, illegal technology transfer and cyber crimes.

The DOD OIG also released a summary of highlights from FY 2019, which also lists the top DOD management challenges for FY 2020.[22] These include, as relating to procurement, improving cyberspace operations, supply chain security and acquisition management ("ensuring that the DOD gets what it pays for on time, at a fair price, and with the right capabilities").

9. Protests Ensure Accountability

The GAO annual report to Congress for FY 2019 released its in November showed the effectiveness rate of bid protests was 44%, the same number as FY 2018 and slightly below the record high numbers in FY 2016 and 2017. The recent effectiveness rates (on average, 45% over the last five years)

indicate that, including agency corrective actions and sustained decisions, a GAO bid protest has a significant chance of resulting in some kind of relief for the protester.

In its November 2019 report, the GAO stated that during FY 2019, it received 2,198 cases, down 16% from 2,607 cases in FY 2018 (and the lowest number of new cases in the past decade). In any given year, DOD procurements can account for more than half of GAO protests.

The DOD has expressed its concerns in recent years over delays brought to its procurement system by bid protests. The January 2019 Volume 3 Report of the Section 809 Advisory Panel included several recommendations relating to the bid protest system, including the elimination of the opportunity to file a second protest at the COFC after filing first at the GAO, the so-called second bite at the apple protest. This proposal, along with others of the Section 809 panel, may resurface in future NDAA bills.

In the meantime, the DOD's highest-profile and highest-dollar procurements are among those most likely to be protested, including at the GAO, the COFC and the U.S. Court of Appeals for the Federal Circuit.

For example, while DOD's $10 billion JEDI cloud services award, announced in October, has been protested at the COFC, an earlier, separate protest concerning the solicitation and its single-prime-vendor structure remains pending at the Federal Circuit, following solicitation protests at the GAO and the COFC.

In another example, **reported by Law360** in April 2019, the U.S. Army announced that it had selected four companies to provide global logistics support services to U.S. forces in the field under the LOGCAP V contract (valued at a maximum $82 billion over 10 years). Following bid protests first at the GAO and next at the COFC,[23] in December 2019, the Army announced it would reconsider the proposals it received, in corrective action related to its price reasonableness determinations.[24]

These examples demonstrate that the DOD's highest profile contract solicitations and awards are most likely to experience protests, which may delay procurement timelines. While it is true that review by the COFC, and by the Federal Circuit, may lengthen the process for any challenged award or solicitation, the availability of review by these courts, as well as by the GAO, enhances the effectiveness, transparency and accountability of the greater procurement system. In the government's system of checks and balances, that review is sometimes most important when applied to the most important procurements.

10. Increased Threat Environment at Home and Abroad

As the new year begins, government contractors face an increased security threat environment abroad, as well as increased cybersecurity threats at home. On Dec. 27, 2019, a U.S. contractor, who was an interpreter for U.S. forces, was killed in an attack on an air base in Kirkuk, Iraq. In the first week of January, a separate attack on a military base in Manda Bay, Kenya took the lives of a U.S. service member and two DOD contractors.

Government contractors have always shared the risk with the DOD in military conflicts abroad, and the recent geopolitical events create an increased security risk environment for contractors as well as U.S. service members and government employees around the world. Recently, the Professional Services Council, or PSC, asked the DOD and the State Department to "increase coordination and improve communications with industry on issues of operational risks and personnel safety for U.S. government contractors, especially those working overseas."[25]

A letter from the PSC to the DOD and the State Department asks them to alert all contractors to the increased threat, and "establish an improved U.S. government process to provide updated threat information regularly and as needed to all contractors."[26] The letter states that "those affected include not only [DOD and DOS] contractors but all contractors performing overseas missions across the U.S. government."[27]

The PSC also "encouraged its members and all affected contractors to take appropriate actions to prepare for the increased threat environment."[28] U.S. government contractors abroad, especially DOD contractors, must take this increased threat environment into account in all aspects of their work and daily lives.

At the same time, government contractors must be aware of increased cybersecurity threats to the U.S. homeland. The U.S. Department of Homeland Security released a bulletin on Jan. 4, 2020, summarizing an increased threat to the U.S. homeland, including concerns over cyber-enabled attacks against critical infrastructure in the United States.

In addition, on Jan. 6, 2020, DHS's Cybersecurity and Infrastructure Security Agency, or CISA, issued an alert to U.S. businesses and the cybersecurity community concerning the potential for an Iranian cyber response in light of the current tensions.

According to the alert, past offensive cyber operations attributed to the Iranian government have targeted a variety of U.S. industries, including financial services, energy, government facilities, chemical, healthcare, critical manufacturing, communications and the defense industrial base. The CISA alert provides "actionable technical recommendations for IT professionals and providers to reduce their overall vulnerability."[29]

The need for careful attention and significant resources devoted to cybersecurity threats is not new for government contractors, and the recent geopolitical events confirm that cybersecurity threats are continuing to increase. Government contractors, including DOD contractors in particular, must devote increasing resources to meet these increasing challenges. Combined with the security threats abroad, the recent events bring new concerns and challenges this year for government contractors at home and around the world.

Joseph R. Berger *is counsel at Thompson Hine LLP.*

Disclosure: Thompson Hine represents one of the parties to the LOGCAP V bid-protest litigation in matters unrelated to those discussed in this article.

This article is reprinted with permission from Portfolio Media. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, Inc., or any of their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

---

[1] https://www.congress.gov/116/crpt/hrpt333/CRPT-116hrpt333.pdf.

[2] https://www.armed-services.senate.gov/imo/media/doc/FY20%20NDAA%20Conference%20Summary%20_%20FINAL.pdf.

[3] See id. at 14.

[4] See id. at 17.

[5] See id. at 8.

[6] See id. at 9, 15-16, 17-18.

[7] See id. at 9.

[8] The latest CMMC developments are available on the OUSD(A&S) website, https://www.acq.osd.mil/cmmc/.

[9] https://www.acq.osd.mil/ae/#/home.

[10] https://aaf.dau.edu/aaf/.

[11] *Space Exploration Technologies Corp. v. United States*,144 Fed. Cl. 433 (2019).

[12] https://www.law360.com/articles/1180426/a-midyear-look-at-dod-gov-t-contract-law-changes.

[13] *Available at* https://www.nscai.gov/home.

[14] https://www.law360.com/articles/1217965/new-ethics-framework-may-draw-ai-firms-to-dod.

[15] https://fas.org/sgp/crs/natsec/R45178.pdf.

[16] Id.

[17] Id.

[18] Id.

[19] https://fas.org/sgp/crs/natsec/R43838.pdf.

[20] https://blog.gao.gov/2019/05/28/federal-government-contracting-for-fiscal-year-2018-infographic/.

[21] https://www.dodig.mil/Reports/Semiannual-Report-to-the-Congress/.

[22] https://media.defense.gov/2019/Dec/03/2002219420/-1/-1/1/DOD%20OIG%20FY%202019%20HIGHLIGHTS.PDF.

[23] *See* Army To Revisit Bids Amid Protests Over $82B Logistics Deal, https://www.law360.com/articles/1226698/army-to-revisit-bids-amid-protests-over-82b-logistics-deal.

[24] Id.

[25] https://www.pscouncil.org/a/News_Releases/2020/PSC_Calls_for_Increased_Coordination_with_Industry_on_Threats.aspx.

[26] https://www.pscouncil.org/a/Resources/2020/PSC_Letter_on_Threats_to_Overseas_Contractors.aspx.

[27] Id.

[28] Id.

[29] Id.