A Midyear Look At DOD Government Contract Law Changes

By Joseph Berger

Law360 (July 22, 2019)— Developments thus far in 2019 relating to government contract law and policy affecting the U.S. Department of Defense continue to reflect constant changes in the broader government contracting legal arena. Given that the DOD is responsible for the lion's share of U.S. government procurement spending, it often takes the lead on, and is the subject of, cutting-edge efforts focused on statutory and regulatory reform and enforcement. This month also marks the 50th anniversary of the Apollo 11 mission, a significant event in the history of the government contracting field, and I discuss that below as well.

Here are several developments this year-to-date in the government contracts arena meriting particular attention, including significant events relating to science and technology:

Cybersecurity

In June, a top Pentagon official released further details on the DOD's Cybersecurity Maturity Model Certification, or CMMC, program and announced that cybersecurity costs will be considered an allowable cost. The DOD special assistant for cyber within the Office of the Under Secretary of Defense for Acquisition and Sustainment, or OUSD(A&S), Katie Arrington, announced details concerning the CMMC in June at a meeting of the Professional Services Council, and again in July at a meeting of the National Defense Industrial Association.

At events with industry representatives, Arrington has explained that the CMMC would become a requirement in DOD procurements through solicitation proposal instructions and evaluation criteria, located in Sections L and M of a request for proposal, or RFP, which will set the required CMMC level — currently expected as levels one through five — for a specific contract.

The CMMC requirements are planned to be included in requests for information, or RFIs, beginning in June 2020 and in RFPs, in September 2020. The OUSD(A&S) will hold a listening tour with industry at various events this July through September. Arrington's presentation highlights the continuing and increasing priority of cybersecurity within the DOD for all DOD procurements.

According to the OUSD(A&S) website, the DOD "recognizes that security is foundational to

acquisition and should not be traded along with cost, schedule, and performance moving forward." According to the OUSD(A&S):

> OUSD(A&S) is working with DOD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC).
>
> The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyberhygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
>
> The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
>
> The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
>
> The intent is for certified independent third-party organizations to conduct audits and inform risk.[1]

The CMMC program as planned by the DOD would be consistent with Section 1634 of the currently pending Senate version of the National Defense Authorization Act, or NDAA, for fiscal year 2020. Section 1634, "Framework to Enhance Cybersecurity of the United States Defense Industrial Base," would establish the "Cybersecurity Maturity Model Certification" for defense industrial base companies, "scoring companies on a rating scale, and requiring certain ratings for contract awards."

Section 1634 would require the secretary of defense to develop a consistent, comprehensive framework by Feb. 1, 2020, which would include "identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors," as well as "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."

The CMMC program can be expected to bring a new enforcement mechanism to cybersecurity that will benefit the security of contractors and the industrial base, as well as help the DOD avoid future losses to cyber breaches. Cybersecurity can also be expected to be among the current and future subjects of increased auditing, False Claims Act complaints and other enforcement.

In May, a district court denied a motion to dismiss a FCA complaint against a major defense contractor alleging violations of the DFARS cybersecurity clause, 252.204-7012, and a related NASA clause. And in June, U.S. Customs and Border Protection suspended a contractor following a high-profile data breach.

These recent events serve as a reminder that, while the new enforcement mechanisms are under development within the DOD, contractors must devote substantial and increasing resources toward compliance with the current cybersecurity regulations, including the comprehensive DFARS cybersecurity requirements, in order to provide solutions that are both effective and compliant.

Artificial Intelligence

The executive order "Maintaining American Leadership in Artificial Intelligence" was issued by the White House on Feb. 11, 2019, and on Feb. 12, the DOD released a summary of the 2018 DOD Artificial Intelligence Strategy. The DOD's AI Strategy "directs the DOD to accelerate the adoption of AI," stating that the DOD is taking "immediate action to realize the benefits of AI," and the DOD will "harness the potential of AI to transform all functions of the Department positively."

The DOD formally launched its new Joint Artificial Intelligence Center, or JAIC, in June 2018, with plans to increase AI and machine learning capabilities for the military and intelligence communities. The JAIC is a focal point for carrying out the DOD AI Strategy, which "will drive the urgency, scale, and unity of effort needed to navigate this transformation."

In February, the DOD also issued new awards for AI research services for the Defense Technical Information Center as part of a broader $28 billion multiple-award contract.

In March, Director of the Defense Innovation Unit Michael Brown testified before the Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, on AI initiatives within DIU, alongside colleagues from JAIC and the Defense Advanced Research Projects Agency, or DARPA, which has pioneered various AI development efforts prior to JAIC and is currently leading the $2 billion "AI Next" campaign.

Brown stated that "AI has the potential to transform how the Department operates at all levels, from business to the battlefield." Further, he stressed the need for DOD to keep its technological edge:

> In the face of competition from China and Russia, the DOD aims to maintain its technological edge through establishing a more decentralized, experimental procurement approach: cultivating a leading AI workforce, engaging academic, commercial and international allies and partners, and developing ethical and lawful guidelines for AI use.

Brown stated that DIU seeks to lower barriers to entry into the defense market by more closely matching commercial terms and contracting speeds and leveraging Other Transaction, or OT, authority. Furthermore, he said that new acquisition processes allow the DOD "to acquire the best commercial technology faster and cheaper than the traditional system," and "new acquisition pathways create more opportunities for national security service, making the DOD a more competitive employer of AI and other sought-after tech talent through commercial contracts."

Artificial Intelligence can be expected to support additional DOD efforts to maintain a U.S. technology edge. In March, the DOD released an updated DOD manual on rapid acquisition authority, detailing its processes for rapidly fulfilling urgent operational needs using RAA. In April, the U.S. Air Force announced a new science and technology strategy, which is intended to improve deployment of "breakthrough technologies" and increase the Air Force's technological advantages over rival militaries.

The DOD's Information Technology Transformation

The DOD's increasing prioritization of cybersecurity and AI is taking place within the fundamental transformation of its enterprise-wide IT infrastructure. In February, the DOD released a new cloud strategy to facilitate its efforts to move its IT functions to the cloud, the "DoD Cloud Strategy," dated December 2018, which noted that the "battlefield exists as much in the digital world as it does in the physical."

According to the strategy, "[c]loud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage." The strategic objectives include exponential growth, the ability to scale for DOD missions, proactively addressing cyber challenges, enabling AI and data transparency, extending tactical support for the warfighter and driving IT reform at the DOD.

A key part of the cloud strategy is the $10 billion Joint Enterprise Defense Infrastructure, or JEDI, cloud contract. JEDI will encompass a variety of DOD data, from the Pentagon to soldiers in the field. The JEDI procurement was protested at the U.S. Court of Federal Claims in December 2018 over its single-prime-vendor structure — and later, alleged conflict of interest.

The DOD announced in April 2019 that it had reached a finding that there was no conflict of interest involving a former DOD employee, and narrowed down the competitive range candidates to Microsoft and Amazon. Earlier this month, the Court of Federal Claims denied Oracle's protest over the JEDI solicitation.

In addition to JEDI, the DOD announced late last year that it would team with the U.S. General Services Administration for its $8 billion office services cloud contract known as the Defense Enterprise Office Solution, or DEOS, which will encompass the military's email and office productivity systems. In April, the GSA issued the request for quotations through its eBuy platform.

While DEOS and JEDI are the largest DOD cloud computing contracts to date, the DOD can be expected to spend additional billions on IT, cloud computing and cybersecurity in the coming years, as well as on AI and machine learning. Major IT awards and protests have continued this year. In April, a Court of Federal Claims decision denied protests over DISA's $17.5 billion multi-award ENCORE III contract for IT services.

In June, the Defense Information Systems Agency, or DISA, awarded 23 contracts to small businesses on a $7.5 billion systems engineering, technology and innovation program, or SETI, to help the DOD improve its IT capabilities — the DOD issued awards to 14 large companies on the program last year. DISA also announced at a cyber industry conference in May that it will seek to issue more OT contracts for innovative technology pilots, including AI and machine learning.

In February, the U.S. Army Cyber Command awarded a $905 million contract for cyberspace operations support, and Law360 reported that the Cyber Command now has 19,000 soldiers and civilians. In May, the Navy awarded nine cyberspace support contracts collectively worth up to $6 billion. As the DOD's spending on IT transformation continues, so will its focus on cybersecurity, and its contractors should expect to devote increasing attention and resources to this critical priority for the DOD.

On July 12, the DOD released a comprehensive digital modernization strategy to guide the DOD IT transformation.[5] "This strategy outlines how the department will increase agility and remain competitive within a constantly evolving digital global threat landscape," according to a July 15 press release quoting DOD Chief Information Officer Dana Deasy.

The strategy is guided by four priorities and framed within four organizing goals. The DOD chief information officer priorities include cybersecurity, AI, cloud and "command, control and communications," or C3. The organizing goals include four strategic initiatives focused on innovation, optimization, resilient cybersecurity and cultivation of talent.

According to the strategy's foreword:

> [O]ur approach is simple. We will increase technological capabilities across the Department and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena.

House and Senate NDAA Bills

On July 12, the U.S. House of Representatives passed a $733 billion NDAA for FY 2020, H.R. 2500, in a vote divided along party lines. The House bill must be reconciled in conference committee with the Senate's $750 billion version, S. 1790, which passed on June 27.

Among the notable provisions of the Senate bill is Title XVI, Subtitle A, which redesignates the Air Force Space Command as the United States Space Force, establishing a commander of the Space Force, an assistant secretary of defense for space policy and a principal assistant to the secretary of the Air Force for space acquisition and integration. Subtitle C contains a number of significant cyberspace-related matters, including a program to improve acquisition of commercial cybersecurity products and services and a study on the future cyber warfighting capabilities of the DOD.

The House bill includes a number of provisions in Title VIII relating to acquisition security, including revised authorities to defeat adversary efforts to compromise U.S. defense capabilities. Consistent with the CMMC cybersecurity model discussed above, the bill states that the DOD "must develop policies and regulations that move security from a cost that defense contractors seek to minimize to a key consideration in the award of contracts, equal in importance to cost, schedule, and performance."

Both the House and Senate bills would provide new authorities for the rapid acquisition of software.

The NDAA bills do not address many of the more revolutionary changes recommended in the January 2019 report of the Section 809 Advisory Panel on Streamlining and Codifying Acquisition Regulations. But the influence of the Section 809 Panel recommendations may be expected to continue in future NDAAs and reform efforts.

Department of Defense contractors can also expect continuing regulatory changes, some of which reflect recommendations of the Section 809 Panel and other reforms previously adopted in prior NDAAs. As of July 12, there were more than 60 open DFARS cases pending and at least 50 open federal acquisition regulation, or FAR, cases, many of which result from the NDAAs of prior years.

Small Business Opportunities

In June, the U.S. Small Business Administration released its annual small business procurement scorecard, indicating that government-wide, federal agencies awarded almost $121 billion in contracts to small businesses in FY 2018, a new record high, amounting to just over 25% of federal prime contract awards.

The DOD's FY2018 scorecard indicates that the DOD awarded just over 24% of its contract awards, or $72 billion, to small businesses — surpassing its goal of 22%. According to the SBA, the DOD accounted for more than $120 billion in prime and subcontract awards to small businesses, while the DOD "developed and continues to refine a Small Business Strategy to ensure a mission focus and grow a robust and capable small business defense industrial base."

These statistics are a reminder of the significant role that small businesses serve in the U.S. economy and as a critical component of the DOD industrial base. Small businesses will be expected to meet the CMMC requirements that will be implemented by the DOD next year throughout the industrial base. According to the DOD, "the goal is for CMMC to be cost- effective and affordable for small businesses to implement at the lower CMMC levels."

Acquisition Authorities and the Moon Landing

The moon landing, 50 years ago last Saturday, serves as a reminder that American science and technology have continued to lead the way and when challenged have leapt forward. In recent years, Congress has increased DOD Other Transaction authorities as a means to help the DOD maintain the U.S. position in global science and

technology leadership. Future NDAAs will likely continue support for expanded authorities for OTs, and the DOD will continue to use them to the maximum extent available.

On Feb. 22, 2019, the Congressional Research Service, or CRS, released an updated report to Congress, "Department of Defense Use of Other Transaction Authority: Background, Analysis, and Issues for Congress." The report noted that in FY2017, the DOD obligated $2.1 billion on prototype OT agreements, representing less than 1% of contract obligations for the year. "However, the use of OTs is expected to grow at a rapid pace, due in part to recent statutory changes expanding other transaction authorities."

As background to the DOD's OT authority, the CRS report provides a short history of the space race, which led to the creation of NASA as well as OT authority:

> On October 4, 1957, the Soviet Union triggered a space race with the United States when it successfully launched Sputnik I into orbit, becoming the first nation to send a man-made satellite into space. Congress, concerned that the United States was falling behind in space, held a series of hearings on an "emergency" effort to respond to the Soviet launch of Sputnik. At the same time, a bill was introduced in the Senate to create an agency with the means to quickly and efficiently develop a national space program. These efforts led to passage of the National Aeronautics and Space Act of 1958 (Space Act ...) in July 1958, which established the National Aeronautics and Space Administration (NASA).[2]

The CRS explained that, in an effort to give the new agency "the necessary freedom to carry on research, development and exploration ... to insure the full development of these peaceful and defense uses without unnecessary delay," the Space Act granted NASA broad authorities to enter into various contracts and "other transactions as may be necessary" to accomplish its mission of research and exploration. This eventually led to similar OT authorities first granted to the DOD in 1990.

The CRS report notes, referring to the Section 809 reports, that "some argue that OTs have particular import today. Drawing parallels to the space race, these analysts argue that the DOD is engaged in a defense technology race." Further, they argue, "OTs and similar rapid acquisition authorities are critical for the DOD to compete in such a fast-paced global environment where technology and innovation are no longer driven by the DOD, but by industry and foreign competitors."[3]

And around the 50th anniversary of the Apollo 11 moon landing, other commentary has pointed out that "NASA didn't achieve Apollo on its own. American business and science helped – on contract." As one history professor said, "as the U.S. charts its spaceflight future, we ought to remember the lessons of the contract in the Apollo business model."[4]

Picking up where the CRS report left off, on May 25, 1961, President John F. Kennedy, in an address to Congress, said that the United States should commit itself to achieving the goal of landing on the

moon within the decade. On Sept. 12, 1962, Kennedy gave a speech before 40,000 people at Rice University in Houston and spoke eloquently about the technological challenges required to send a rocket to the moon and to return safely to Earth. And to "do all this, and do it right, and do it first before this decade is out," he said, "then we must be bold." President Kennedy's vision was realized 50 years ago when Apollo 11 sent humans to the moon. Commander Neil Armstrong and pilot Buzz Aldrin landed in the Apollo Lunar Module, Eagle, on July 20, 1969, and hours later, Armstrong became the first person to walk on the lunar surface.

In May 2019, NASA awarded contracts in support of one of the first steps in its current exploration plans: To demonstrate power, propulsion and communications capabilities for NASA's lunar gateway, the planned lunar orbiting staging point to return astronauts to the moon's surface. NASA is currently working on the Artemis program to establish a sustainable presence on the moon, send the next man and first woman to the moon as soon as five years from now and prepare for NASA's longer-term mission to send humans to Mars.

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

[1] https://www.acq.osd.mil/cmmc/index.html

[2] CRS Report at 1 (available at https://crsreports.congress.gov/product/pdf/R/R45521).

[3] CRS Report at 7.

[4] https://www.marketwatch.com/story/the-business-lesson-from-apollo-11-that-we-shouldnt-forget-2019-07-15

[5] https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF