THIS YEAR'S MOST IMPORTANT CHANGES IN **GOVERNMENT CONTRACT LAW AND POLICY** (SO FAR)

BY THE GOVERNMENT CONTRACTS PRACTICE GROUP
AT DRINKER BIDDLE & REATH LLP

As we all know, the areas of U.S. federal government contract law and policy are constantly developing and changing. Keeping us on our toes, changes come from all three branches of our government: Congress issues new laws, Executive Branch departments and agencies issue new regulations and policies, and courts and boards issue new decisions to expand the body of case law.

It may come as no surprise that, thus far in 2019, developments in government contracts law and policy have occurred in several areas that seem to be perennial favorites for changes (e.g., the False Claims Act, the Truthful Cost or Pricing Data statute, and in the area of commercial items). However, several important developments have also occurred in hot emerging areas (e.g., cybersecurity, supply chain security, and artificial intelligence) and even in areas where changes rarely occur (e.g., definitization of contracts and Buy American statute requirements). Finally, in 2019, government contract litigation has provided some areas of clarification (and mostly hope) for contractors.

This article highlights the most important developments in government contract law and policy in 2019.[1]

THE FALSE CLAIMS ACT CONTINUES TO EVOLVE

DOJ Guidelines on Cooperation Credit

In May 2019, the Department of Justice (DOJ) published formal guidelines[2] for determining the credit to be provided to contractors cooperating in False Claims Act[3] investigations as a section of DOJ's Justice Manual.[4] The guidelines identify the three primary actions DOJ views as "cooperation":

- Voluntary disclosure of the conduct that potentially violates the False Claims Act,
- Cooperating with the government's investigation, and
- Taking remedial action.

Perhaps most helpful, the guidelines provide specific examples of what DOJ deems to be "cooperating with an investigation," including:

- Identifying employees involved in the conduct,
- Obtaining and disclosing information to the government that goes beyond what is required by law,
- Disclosing facts uncovered through an internal investigation, and
- Admitting liability and accepting responsibility for the misconduct.

While the guidelines help clarify what DOJ expects concerning "cooperation," they also raise some troubling questions for contractors. Most troubling, the DOJ will only credit as "cooperation" the voluntary disclosure of information "not required by law." Taken literally, this policy would not credit disclosures under the mandatory disclosure rule as cooperation, which would effectively eliminate any possibility for government contractors to receive credit for disclosures to the government. Also, the means for determining whether a contractor has accepted responsibility and liability is always a hot button. Contractors and DOJ could reasonably disagree over the appropriate enforcement action, and DOJ could presumably view this disagreement as a lack of cooperation. Thus, a contractor that has disclosed all conduct and information, cooperates with the investigation fully according to the guidelines, but disagrees in good faith that the conduct amounts to fraud, will apparently not be viewed as a cooperator under this third element because it will not accept the government's assessment.

DOJ Guidance on Compliance Programs

Also in May 2019, the DOJ provided guidance to prosecutors, and in doing so, to contractors, on evaluating the effectiveness of corporate compliance programs. DOJ will consider the effectiveness of contractor compliance programs in determining whether and what to charge criminally, the appropriate resolution, the penalty, and what compliance obligations will be imposed as part of any criminal resolution.[5] DOJ's analysis focuses on whether the compliance program is designed well, has been implemented in good faith and effectively, and is working. The review will include not only the written policies but also the procedures for implementing the policies, training, and communication within the organization; procedures for review and improvements; reporting structure; investigation procedures; due diligence; and management commitment.

Although directed at criminal cases, the guidance will likely guide DOJ's review of compliance programs in any enforcement action, including investigations and proceedings under the False Claims Act. Contractors should take advantage of this insight to review their own compliance programs.

False Claims Act Statute of Limitation Clarified, and Not in a Good Way for Contractors

As contractors unfortunate enough to have experience with the False Claims Act know very well, the False Claims Act has two alternative limitations periods:

- Six years from the offending conduct, or
- Three years from when a government official "charged with responsibility to act" first learns of the offending conduct but no more than 10 years.[6]

Federal courts of appeals had split on whether the alternative "government knowledge" limitations period applied to cases where the government did not intervene to join the case. Some found that the "government knowledge" alternative applied only to the government because it expressly applies to government officials charged with responsibility to act. Others allowed *qui tam* relators to invoke the "government knowledge" alternative even when the government did not intervene.

On May 13, 2019, the Supreme Court issued a decision in *Cochise Consultancy Inc., v. United States ex rel. Hunt*,[7] siding with the courts of appeals that allowed relators to invoke the government knowledge limitations period even when the government does not intervene. Relying on the "plain text" of the False Claims Act, the Court found nothing in the statute limited the alternative limitations period to the government. Importantly, the Court made clear that the relator is not an "official" that triggers the government knowledge because the relator is neither an official nor employee of the United States. Thus, even when invoked by a relator, the alternative limitations period is triggered by the knowledge of the appropriate government official (not the relator). The Supreme Court declined to clarify whether the Attorney General is the only official of the United States "charged with responsibility to act" (as argued by the government) or whether another official or employee could trigger the alternative limitations period.

The bottom line is that contractors must contend with the alternative 10-year limitations period even when the government does not intervene, which is an unwelcome development.

The False Claim Act Reaches Cybersecurity

The government has been developing its cybersecurity requirements for years, and contractors have been struggling to understand and comply with them. Given the breadth of potential False Claims Act liability (arguably imposing liability for any knowing violation of a material statutory, regulatory, or contractual obligation), it may have been only a matter of time until either the government or a *qui tam* relator would attempt to impose liability for noncompliance with cybersecurity requirements. Well, the time has arrived.

United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.

On October 29, 2015, a *qui tam* relator filed a complaint against Aerojet Rocketdyne, Inc. (AR), a wholly-owned subsidiary of Aerojet Rocketdyne Holdings, Inc. (ARH), alleging fraud against the government under the False Claims Act, among other claims, in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*[8] AR and ARH manufacture propulsion systems for both deep space missions and orbiting satellites in support of the space industry, and for missiles and missile defense systems in support of the defense industry, with key customers including the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA). Between 2014 and 2016, AR entered into at least six contracts with DOD, and nine contracts with NASA.

On June 5, 2018, the government declined to intervene in the relator's case against AR. AR filed a motion to dismiss against the relator, and the relator opposed the motion to dismiss.

For purposes of the motion, AR appears to have acknowledged that it was not fully compliant with the cybersecurity terms of its DOD and NASA contracts. AR argued that the False Claims Act case should be dismissed because its noncompliance was not "material"—i.e., its cybersecurity noncompliance did not meet the materiality element of the False Claims Act under *Universal Health Services., Inc. v. United States ex rel. Escobar*[9] for four reasons:

1 | AR had fully disclosed its noncompliance with the cybersecurity terms to its government customers, including through a letter dated September 18, 2014. The government would not have contracted with AR after the disclosure of noncompliance if compliance was material.

2 | The government continued to contract with AR and did not intervene in the case after investigating AR's noncompliance. The government would have stopped contracting with AR and intervened to support the relator after it investigated AR's noncompliance if compliance was material.

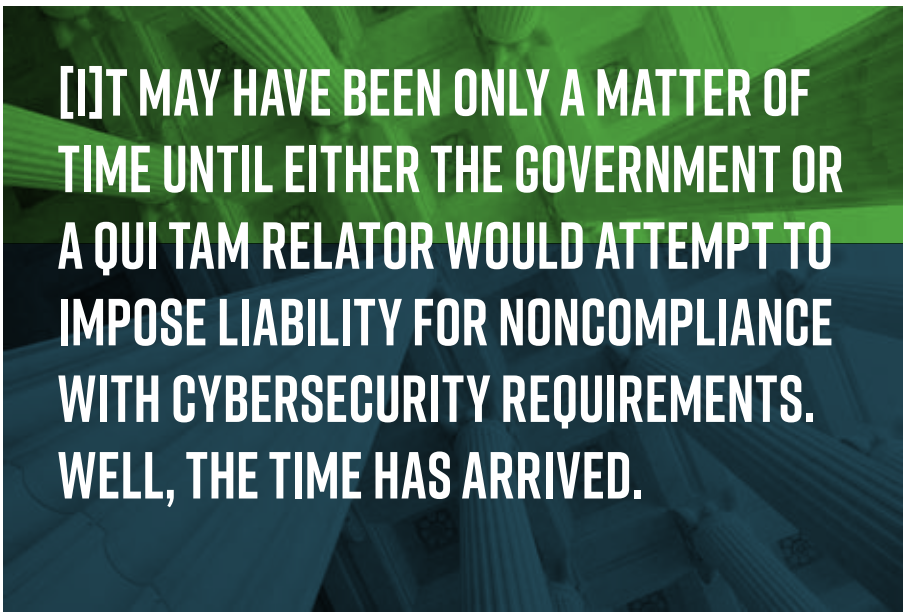
3 | The noncompliance did "not go to the central purpose of any of the contracts, as the contracts pertain to missile defense and rocket engine technology, not cybersecurity."[10] A term that was not necessary to the central purpose of the contract could not be material.

4 | The government "never expected full technical compliance" by industry and "constantly amended its acquisition regulations and promulgated guidance that attempted to ease the burdens on the industry."[11] The government understood the difficulty of compliance and was working with industry to get compliance; therefore, noncompliance could not be material.

The Court rejected all of AR's arguments in support of its motion to dismiss. First, the Court concluded that AR's disclosure could be proven false—it was incomplete and misleading.

Second, the government could have declined to intervene for a host of reasons—lack of resources, for one—that had nothing to do with whether it viewed cybersecurity compliance as material. The appropriate inquiry, according to the Court, was "whether AR's alleged misrepresentations were material *at the time* the government entered into or made payments on the relevant contracts."[12]

Third, although the contracts were for missile and rocket engine technology, "misrepresentations as to compliance with…cybersecurity requirements could have influenced the extent to which AR could have performed the work"[13] required by the contracts. Even though cybersecurity was not the central purpose



of the contract, it could still be a material requirement under the False Claims Act.

Fourth, the Court appeared to accept AR's argument that the government did not expect full compliance with the cybersecurity terms, as demonstrated by the government's numerous changes to the requirements. The Court concluded, however, that "even if the government never expected full technical compliance," the extent of noncompliance could have "still mattered to the government's decision to enter into a contract."[14]

The Court concluded that the relator had alleged sufficient facts to permit his case to proceed in the litigation and denied AR's motion to dismiss. AR would have to defend its cybersecurity compliance in the case, at least through discovery and potentially trial. Thus, the *Markus* case demonstrates that potential relators (and their counsel) are willing to sue contractors under the False Claims Act for cybersecurity noncompliance, regardless of the government's recognition of the complexity of compliance with cybersecurity requirements, and at least one Court was willing to conclude that *the degree* of cybersecurity noncompliance could serve as the basis for a False Claims Act case.

United States, ex rel. Glenn v. Cisco Sys. Inc.

Cybersecurity requirements played a more direct role in another *qui tam* case that resulted in a settlement. In *United States, ex rel. Glenn v. Cisco Sys. Inc.*,[15] a *qui tam* relator alleged that Cisco Systems delivered software for video feeds with weaknesses that could permit a hacker access. In July 2019, Cisco Systems agreed to pay $8.6 million to settle the suit, making clear, however, that it did not agree that the weaknesses existed, and that no hacking had actually occurred.

The *Cisco Systems* settlement makes clear that allegations of cybersecurity violations—even where no cyber incident has occurred—expose a contractor to liability.

CYBERSECURITY IS MOVING QUICKLY

DCMA to Audit DOD Cybersecurity Compliance

On January 21, 2019, the under secretary of defense for acquisition and sustainment issued a memorandum[16] establishing procedures to implement the cybersecurity requirements of *Defense Federal Acquisition Regulation Supplement* (*DFARS*) 252.204-7012 and National Institute of Standards and Technology (NIST) SP 800-171 by directing the Defense Contract Management Agency (DCMA) "to validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7001." As part of its review of purchasing systems, DCMA was directed to review:

- "Contractor procedures to ensure contractual DOD requirements for marking and distribution statements on DOD [controlled unclassified information (CUI)] flow down appropriately to their Tier 1 Level Suppliers"[17]; and
- "Contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171."[18]

On February 26, 2019, DCMA updated its *Contractor Purchasing System Review Guidebook* to incorporate requirements from the January 2019 memorandum. DCMA noted that "[p]rotecting [CUI] is a critical aspect" of the supply chain management process.

Audit and enforcement of cybersecurity requirements within DOD is now clear: It will be conducted by DCMA.

DOD Will Develop Cybersecurity Maturity Model Certification

In March 2019, DOD began creating the Cybersecurity Maturity Model Certification (CMMC) program,[19] intended to be "a unified cybersecurity standard for DOD acquisitions to reduce exfiltration of [CUI] from the Defense Industrial Base…."[20] The CMMC effort will build "upon existing regulation [i.e., DFARS 252.204-7012] that is based on trust by adding a verification component with respect to cybersecurity requirements," and will "review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced."[21] Contractors will receive a certification based on their levels of compliance by third-party certifiers.

NCMA EVENTS

Connecting to Create What's Next

NCMA offers in-person events on a variety of topics to help you enhance your career and your organization's performance. Attending an in-person event is a great way to learn new information, meet new contacts, and earn CPE/CLP credits. Here are our upcoming events.

GOVERNMENT CONTRACT MANAGEMENT SYMPOSIUM

December 9–10, 2019

GCMS 2019 GOVERNMENT CONTRACT MANAGEMENT SYMPOSIUM DECEMBER 9-10 ARLINGTON, VA

NCMA's 38th Annual Government Contract Management Symposium (GCMS) is held annually in the DC metro area and provides training for 1,000+ professionals in both government and industry contracting. This must-attend event features main stage discussions from senior acquisition leaders, breakout sessions on contracting hot topics, and many networking opportunities.

Hyatt Regency Crystal City
Arlington, VA

CPE 14 Hours

SUBCON TRAINING WORKSHOPS

April 1-2, 2020

SubCon TRAINING WORKSHOPS APRIL 1-2, 2020 • TYSONS, VA

NCMA's SubCon Training Workshops (SubCon) provides comprehensive subcontracts training led by experienced practitioners. Join 200+ industry procurement professionals and government buyers and program managers for two days of training in the format of your choice. Choose to spend a full day in a single-topic immersion workshop or four breakout sessions on multiple topics.

The Ritz-Carlton
Tysons, VA

CPE 12 Hours

WORLD CONGRESS 2020

July 26–29, 2020

WORLD '20 CONGRESS GAYLORD TEXAN JULY 26–29

NCMA's World Congress is the nation's premier education event for contract management, procurement, and acquisition professionals. Over 2,000 participants from all career levels in government and industry gather each year to advance their knowledge and connect with peers. This four-day event is packed with educational content and networking opportunities. You won't want to miss it!

Gaylord Texan
Grapevine, TX

CPE 20 Hours

ncmahq.org/events

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION
CONNECTING TO CREATE WHAT'S NEXT

DOD intends to release a final CMMC program by January 2020 and begin including requirements for offerors to possess CMMCs in requests for information in June 2020 and in requests for proposals in the Fall of 2020.

NIST Issues Additional Cybersecurity Guidance for High-Value Assets and Critical Programs

On June 19, 2019, NIST issued for comment SP 800-171 Rev. 2,[22] "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," which NIST described as primarily editorial and organizational changes to the prior version (Rev. 1). Along with Rev. 2, NIST released SP 800-171B, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets."[23] NIST drafted SP 800-171B in response to "an ongoing barrage of serious cyber-attacks" on DOD,[24] and DOD's request to NIST for additional guidance for "high value assets" or "critical programs" that that have been subjected to advanced persistent threats.

NIST's enhanced security requirements provide a "new multidimensional, defense-in-depth protection strategy that includes three, mutually supportive and reinforcing components." These components include:

- Penetration-resistant architecture,
- Damage-limiting operations, and
- Designing for cyber resiliency and survivability.

NIST also released a DOD cost estimate, "Request for Comments on Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations—Enhanced Security Requirements for Critical Programs and High Value Assets,"[25] which analyzes costs of implementing and maintaining SP 800-171B.

Special Emergency Procurement Authority for Cyber-Attacks and Other Emergencies

On May 6, 2019, DOD, the General Services Administration (GSA), and NASA issued a final rule to implement Sections 816 and 1641 of the National Defense Authorization Act (NDAA) for Fiscal Year 2017.[26] Sections 816 and 1641 modify 41 USC 1903, "Special Emergency Procurement Authority," to establish special emergency procurement authorities to allow for a higher micro-purchase threshold (MPT) and simplified acquisition threshold (SAT) for acquisitions of supplies or services that—

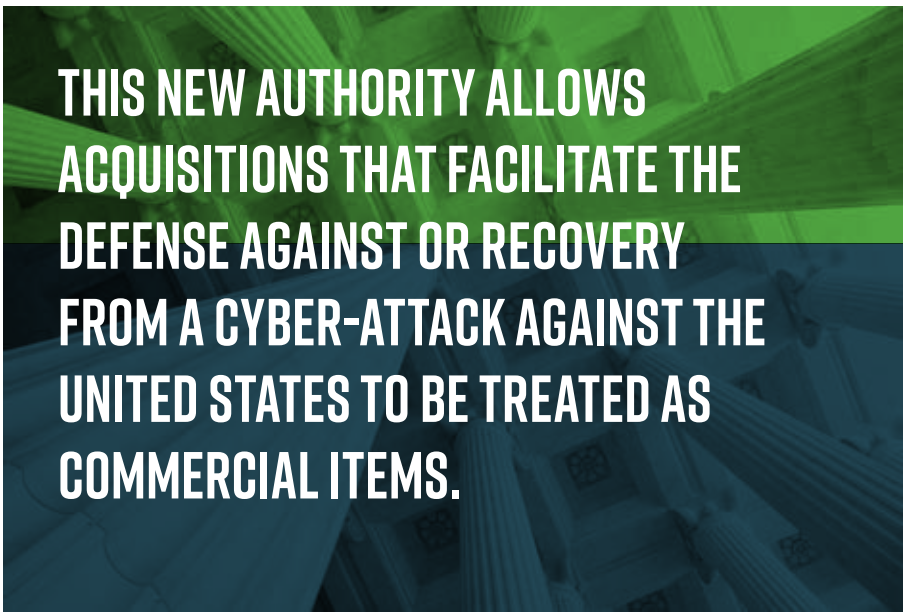
- Facilitate defense against or recovery from cyber-attack,
- Support a request from the Secretary of State or the Administrator of the U.S. Agency for International Development to facilitate provision of international disaster assistance pursuant to 22 USC 2292 *et seq*., or
- Support responses to an emergency or major disaster.[27]

This new authority allows acquisitions that facilitate the defense against or recovery from a cyber-attack against the United States to be treated as commercial items.

Acquisitions with an estimated value between the MPT and SAT and the higher thresholds for the expanded special emergency procurement authorities will use simplified procedures, thereby reducing the requirements imposed on offerors when responding to the solicitation. The rule became effective June 5, 2019.

DOD Expands Cybersecurity Restrictions on Foreign Satellite Services

On May 14, 2019, DOD issued a final rule to implement Section 1603 of the 2018 NDAA[28] for and Section 1296 of the 2017 NDAA. Section 1603 imposes additional prohibitions regarding acquisition of certain foreign commercial satellite services, such as cybersecurity risk and the source of satellites and launch vehicles used to provide the foreign commercial satellite services. Section 1603 also expands the definition of "covered foreign country" to include Russia. Section 1296 prohibits the purchase of items from a Communist Chinese military company. The final rule modifies the clauses at DFARS 252.225-7007, "Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies," and 252.225-7049, "Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign



Entities—Representation." The rule became effective on May 31, 2019.

The Government Applies Cybersecurity Restrictions to Foreign Telecommunications and Video Surveillance Equipment and Services

On August 13, 2019, DOD, GSA, and NASA issued an interim rule amending the *Federal Acquisition Regulation* (*FAR*) to implement Section 889(a)(1)(A) of the 2019 NDAA.[29] Section 889(a)(1)(A) prohibits agencies from procuring, obtaining, or extending/renewing a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system.

"Covered telecommunications equipment or services" is defined in the statute to mean:

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- For the purpose of public safety, security of U.S. government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- Telecommunications or video surveillance services provided by such entities or using such equipment; or
- Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Under the interim rule, contracting officers must include the provision at FAR 52.204-24, "Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment," and the corresponding clause at FAR 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," in all solicitations issued on or after August 13, 2019, and resultant contracts, and in all solicitations issued before August 13, 2019 (provided award of the resulting contract(s) occurs on or after August 13, 2019). Under certain circumstances, an agency may grant a one-time waiver on a case-by-case basis for up to a two-year period. The interim rule also requires submission of a representation with each offer that will require offerors to identify as part of their offer any covered telecommunications equipment or services that will be provided to the government.

The Government Finalizes Cybersecurity Restrictions on Kaspersky Lab Products or Services

On September 10, 2019, DOD, GSA, and NASA adopted as final, without change, an interim rule amending the *FAR* to implement Section 1634 of the 2018 NDAA. The interim rule amended FAR Part 4, adding a new Subpart 4.20, "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab," with a new corresponding contract clause at 52.204-23, "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities." The interim rule also added text in FAR Subpart 13.2, "Actions at or Below the Micro-Purchase Threshold," to address Section 1634 with regard to micro-purchases. To implement Section 1634, the clause at 52.204-23 prohibits contractors from providing any hardware, software, or services developed or provided by Kaspersky Lab or its related entities, or using any such hardware, software, or services in the development of data or deliverables first produced in the performance of the contract. The contractor must also report any such hardware, software, or services discovered during contract performance—and this requirement flows down to subcontractors as well. The rule became effective September 10, 2019.

The Navy Modifies Its *FAR* Supplement to Address Cybersecurity Requirements on Critical Programs

Implementing the procedures set forth by the Assistant Secretary of the Navy (Research, Development, and Acquisition) in a memorandum issued September 28, 2018,[30] the U.S. Navy revised the *Navy Marine Corps Acquisition Regulation Supplement* (*NMCARS*) in September 2019 to impose enhanced cybersecurity controls on critical programs. Specifically, Annex 16 was added to the *NMCARS*, which includes language that must be included in solicitations and contracts where the risk to a critical program and/or technology warrants its inclusion. The Navy also directs contracting officers to address a contractor's failure to comply with the Annex 16 and DFARS 252.204-7012 by reducing the contract price or reducing or suspending progress payments in NMCARS Subpart 5204.73.

THE GOVERNMENT'S DEVELOPING ARTIFICIAL INTELLIGENCE STRATEGY

DOD's Strategic Approach to AI

In 2019, the government took two significant steps in developing a cybersecurity strategy. On February 12, 2019, DOD released a "Summary of the 2018 Department of Defense Artificial Intelligence Strategy,"[31] which recognizes the importance of AI to the national defense. The Summary states:

> [DOD's] Artificial Intelligence (AI) Strategy directs the DOD to accelerate the adoption of AI and the creation of a force fit for our time. A strong, technologically advanced Department is essential for protecting the

> security of our nation, preserving access to markets that will improve our standard of living, and ensuring that we are capable of passing intact to the younger generations the freedoms we currently enjoy.
>
> AI is rapidly changing a wide range of businesses and industries. It is also poised to change the character of the future battlefield and the pace of threats we must face. We will harness the potential of AI to transform all functions of the Department positively, thereby supporting and protecting U.S. service members, safeguarding U.S. citizens, defending allies and partners, and improving the affordability, effectiveness, and speed of our operations. The women and men in the U.S. armed forces remain our enduring source of strength; we will use AI-enabled information, tools, and systems to empower, not replace, those who serve.[32]

DOD identified five components of its strategic approach:

- "Delivering AI-enabled capabilities that address key missions";
- "Scaling AI's impact across DOD through a common foundation that enables decentralized development and experimentation";
- "Cultivating a leading AI workforce";
- "Engaging with commercial, academic, and international allies and partners"; and
- "Leading in military ethics and AI safety."[33]

DOD also tasked the "Joint Artificial Intelligence Center (JAIC) to accelerate the delivery of AI-enabled capabilities, scale the Department-wide impact of AI, and synchronize DOD AI activities to expand Joint Force advantages."[34]

NIST's Plan for AI Implementation Across Government

On August 9, 2019, NIST released "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools."[35] This release was in response to Executive Order 13859,[36] which had directed NIST to issue "a plan for federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies."[37] The plan identifies the following focus areas for AI standards:

- Concepts and terminology,
- Data and knowledge,
- Human interactions,
- Metrics,
- Networking,
- Performance testing and reporting methodology,
- Safety,
- Risk management, and
- Trustworthiness.[38]

NIST recommends that "[s]tandards should be complemented by related tools to advance the development and adoption of effective, reliable, robust, and trustworthy AI technologies."[39] Such tools may include the following:

- Data sets in standardized formats, including metadata for training, validation, and testing of AI systems;

- Tools for capturing and representing knowledge and reasoning in AI systems;
- Fully documented use cases that provide a range of data and information about specific applications of AI technologies and any standards or best practice guides used in making decisions about deployment of these applications;
- Testing methodologies to validate and evaluate AI technologies' performance;
- Metrics to quantifiably measure and characterize AI technologies;
- Benchmarks, evaluations, and challenge problems to drive innovation;
- AI testbeds; and
- Tools for accountability and auditing.[40]

NIST also recommends that the federal government take the following steps as part of a "deeper, consistent, long-term engagement in AI standards development activities to help the United States to speed the pace of reliable, robust, and trustworthy AI technology development"[41]:

- Bolster AI standards-related knowledge, leadership, and coordination among federal agencies to maximize effectiveness and efficiency;
- Promote focused research to advance and accelerate broader exploration and understanding of how aspects of trustworthiness can be practically incorporated within standards and standards-related tools;
- Support and expand public-private partnerships to develop and use AI standards and related tools to advance reliable, robust, and trustworthy AI; and
- Strategically engage with international parties to advance AI standards for U.S. economic and national security needs.[42]

THE GOVERNMENT KEEPS TINKERING WITH COMMERCIAL ITEMS

DOD Encourages the Use of Commercial or Non-Government Standards and Specifications

On February 15, 2019, DOD issued a final rule to implement Section 875(c) of the 2017 NDAA, which requires *DFARS* revisions "to encourage offerors to propose commercial or non-government standards and industry-wide practices that meet the intent of military or government-unique specifications and standards."[43] This rule amends DFARS 211.107(b) to require the use of FAR 52.211-7, "Alternatives to Government-Unique Standards," in solicitations that include military or government-unique specifications and standards. Previously, use of this provision was optional in DOD solicitations. Acquisitions valued at or below the SAT are included in this requirement. DOD solicitations for commercial item acquisition, however, are excluded; as such contracts should not include military or government-unique specifications or standards.

Affected contractors who choose to propose alternative standards should remember that the offeror retains responsibility to demonstrate how the alternative standards meet DOD mission requirements.

DOD Requires Justification and Approval for Use of "Brand Name or Equal" Descriptions in Solicitations

On May 31, 2019, DOD issued a final rule[44] to amend DFARS 211.104 and DFARS 211.170 to restrict the use of "brand name or equal" descriptions in solicitations, implementing Section 888(a) of the 2017 NDAA. The final rule requires that competition on DOD contracts not be limited through the use of "brand name or equal" descriptions, or proprietary specifications or standards in solicitations,

unless a justification for such specification is provided and approved in accordance with 10 USC 2304(f). The final rule applies when using sealed bidding procedures, negotiated procedures, or simplified procedures for certain commercial items. The rule became effective May 31, 2019.

DOD Prioritizes Certain Commercial Services

On August 9, 2019, DOD issued a final rule to partially implement Section 876 of the 2017 NDAA.[45] Section 876 requires revision of the guidance issued pursuant to Section 855 of the 2016 NDAA[46] and provides that a contracting officer may not enter into a contract above the SAT for facilities-related services, knowledge-based services (except engineering services), medical services, or transportation services that are not commercial services, unless the appropriate official determines in writing that no commercial items are suitable to meet the agency's needs. The final rule provides different approval levels for contracts that exceed $10 million and those that exceed the SAT but do not exceed $10 million. A new *DFARS* section–212.272, "Preference for Certain Commercial Products and Services," implements the requirements of Section 876. A cross-reference to the new section was also added at DFARS 237.102. The rule became effective August 9, 2019.

GSA Continues to Make Progress in Its Schedule Consolidation

This year, GSA made significant progress in consolidating its 24 Multiple Award Schedules into a single Schedule, an effort initially announced on November 27, 2018. On September 30, 2019, GSA released the solicitation for the consolidated Schedule on FedBizOpps. GSA anticipates transitioning contracts currently under the previous Schedule after a mass modification in 2020.

SOME DEVELOPMENTS IN COST OR PRICING DATA

A Reasonable Expectation of Competition No Longer Constitutes Adequate Price Competition for DOD, NASA, and the Coast Guard

On June 12, 2019, DOD, GSA, and NASA issued a final rule revising the standard for "adequate price competition" applicable to DOD, NASA, and the U.S. Coast Guard, as required by Section 822 of the 2017 NDAA.[47] Section 822 addresses the exception from certified cost or pricing data requirements when prices are based on adequate price competition. The final rule excludes from the standard for adequate price competition those situations in which competition is expected, but only one offer is received. The standard of adequate price competition that is based on a reasonable expectation of competition is now applicable only to agencies other than DOD, NASA, and the Coast Guard.

The final rule became effective July 12, 2019, and implements these changes through revisions to FAR 15.305, 15.403-1, and 15.404-1.

Cost or Pricing Data Required by DOD, NASA, and the Coast Guard When Only One Offer Received in Response to a Competitive Solicitation

On June 28, 2019, DOD issued a final rule[48] to amend the *DFARS* to partially implement Section 822 of the 2017 NDAA to:

- Address the potential requirement for additional cost or pricing data when only one offer is received in response to a competitive solicitation, and
- Make prime contractors responsible for determining whether a subcontract qualifies for an exception from the requirement for submission of certified cost or pricing data based on adequate price competition.

This *DFARS* rule supplements the *FAR* rule previously discussed,[49] which modified the standards for adequate price competition at FAR 15.403-1(c) for DOD, NASA, and the U.S. Coast Guard. The *DFARS* rule became effective July 31, 2019.

NEW RULES FOR DEFINITIZING CONTRACTS

On August 9, 2019, DOD issued a final rule[50] to amend DFARS Parts 215 and 217 to implement Section 811 of the 2017 NDAA and Section 815 of the 2018 NDAA. Section 811 modifies restrictions on undefinitized contract actions (UCAs) regarding risk-based profit, time for definitization, and foreign military sales. Section 815 establishes limitations on unilateral definitizations of UCAs over $50 million. The final rule will make the following changes to the *DFARS*:

- If a UCA is definitized after the end of the 180-day period beginning on the date the contractor submits a qualifying proposal, the head of the agency must ensure profit reflects the cost risk of the contractor as such risk existed on the date the contractor submitted the qualifying proposal.
- The definitization of a UCA may not be extended by more than 90 days beyond the maximum 180-day definitization schedule negotiated in the UCA without a written determination by the secretary of the military department concerned, the head of the defense agency concerned, the commander of the combatant command concerned, or the Under Secretary of Defense for Acquisition and Sustainment, that it is in the best interests of the military department, the defense agency, the combatant command, or DOD, respectively, to continue the action.
- DOD contracting officers may not enter into a UCA for a foreign military sale unless–
  - The contract action provides for definitization within 180 days, and
  - The contracting officer obtains

approval from the head of the contracting activity.
The head of the agency may waive this requirement, if necessary, to support a contingency, humanitarian, or peacekeeping operation.

- Contracting officers may not unilaterally definitize a UCA with a value greater than $50 million until–
  - The end of the 180-day period beginning on–
    1 | The date on which the contractor submits a qualifying proposal to definitize the contractual terms, specifications, and price; or
    2 | The date on which the amount of funds expended under the contractual action is equal to more than 50% of the negotiated overall not-to-exceed price for the contractual action;
  - The service acquisition executive for the military department that awarded the contract (or the Under Secretary of Defense for Acquisition and Sustainment if the contract was awarded by a defense agency or other DOD component), approves the definitization in writing;
  - The contracting officer provides a copy of the written approval to the contractor; and
  - The end of a 30-day period beginning on the date on which the contractor received written approval.

The rule became effective August 9, 2019.

SUPPLY CHAIN AND SOURCING REMAIN IN FOCUS

DOD Makes Supply Chain Risk Management Requirements Permanent

On February 15, 2019, DOD issued a final rule[51] to implement Section 881 of the 2019 NDAA, which made the DFARS Subpart 239.73 requirements for supply chain risk management permanent by removing the sunset provision of the existing regulation, and instead establishing authority under 10 USC 2239a. This *DFARS* rule makes permanent the requirement for DOD contractors to mitigate supply chain risk in the provision of supplies to the government, and DOD's authority to use supply chain risk as an evaluation factor "in information technology procurements for services or supplies as a covered [national security] system, as a part of a covered [national security] system, or in support of a covered [national security] system."[52]

President Trump Directs a Change to the Buy American Statute Calculation

On July 15, 2019, President Donald Trump signed Executive Order 13881,[53] which directed the FAR Council to begin the process of amending the *FAR* so that the following are considered of "foreign origin" under the Buy American statute[54]:

- Iron and steel end products, if the cost of foreign iron and steel used in such iron and steel end products constitutes 5% or more of the cost of all the products used in such iron and steel end products; or

- All other end products, if the cost of the foreign products used in such end products constitutes 45% or more of the cost of all the products used in such end products.

In addition, the Executive Order directs an amendment to the *FAR* that would change the percentage to be added to foreign offers for determining price reasonableness under FAR 25.105 from 6% and 12% to 20% (for other than small businesses) or 30% (for small businesses).

LITIGATION BRINGS HOPE

The Court of Federal Claims Confirms That the Government Must Base a Termination for Default on an Objective Determination Based on Tangible Evidence

In June 2019, the Court of Federal Claims issued a decision, *Alutiiq Manufacturing Contractors*,[55] that offers protection to contractors from termination for default. The termination for default in the *Alutiiq* case resulted from "hostility towards the contractor among the government's contract management personnel," which, in turn "gave [the contractor] no real chance to implement a more rapid schedule," and caused the government to ignore "important sections of the [*FAR*]" in reaching its termination decision.[56] Relying on the decision of the Court of Appeals for the Federal Circuit in *Lisbon Contractors, Inc.*,[57] the Court of Federal Claims confirmed that the government must base a default termination on an objective determination of whether the contractor has a reasonable likelihood of completing performance based on "tangible, direct evidence reflecting the impairment of timely completion."[58]

In essence, *Alutiiq* established that a government contract cannot be terminated based on either a subjective opinion or an analysis lacking tangible, direct evidence.

Contractors Do Not Have to Show Substantial Competitive Harm to Protect "Confidential" Information under the Freedom of Information Act

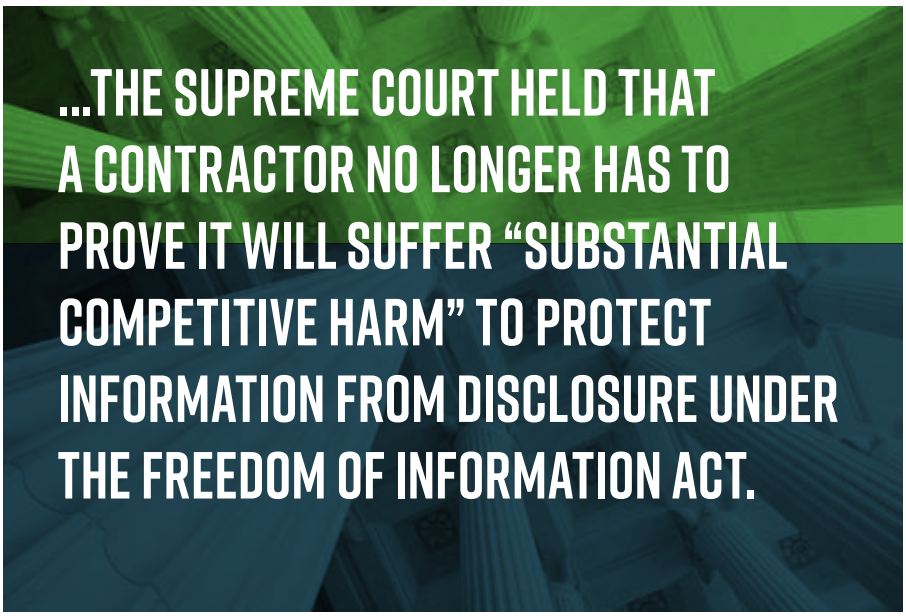
In a decision issued in June 2019 (*Food Marketing Institute*[59]), the Supreme Court held that a contractor no longer has to prove it will suffer "substantial competitive harm" to protect information from disclosure under the Freedom of Information Act (FOIA).[60] Prior to the Supreme Court's decision, many lower courts followed the analysis set forth in the D.C. Circuit's *National Parks & Conservation Assn. v. Morton* case,[61] which incorrectly concluded that under FOIA's "Exemption 4," commercial or financial information is considered "confidential" *only* if disclosure of the information is likely to–

- "[I]mpair the government's ability to obtain necessary information in the future," or

- "[C]ause substantial harm to the competitive position of the person from whom the information was obtained."[62]

The Supreme Court refused to narrow Exemption 4 by adding limitations, such as "substantial harm," which are not expressly required in the statute. Instead, information provided to a federal agency qualifies as "confidential" under the ordinary meaning of the term–i.e., when a contractor customarily maintains the information as "private," or at least "closely held."

The Supreme Court's ruling in the *Food Marketing Institute* case is good news for government contractors. A contractor seeking to protect its commercial or financial information provided to the government will no longer have to prove "substantial competitive harm" to qualify for FOIA Exemption 4. Showing that the contractor customarily maintains the information as "private"/"closely held" should be sufficient to establish the information as "confidential" under FOIA Exemption 4.



A FINAL WORD

As this summary demonstrates, at least for 2019, the legal and policy landscape of government contracts is ever-changing. Needless to say, keeping abreast of the changes in government contract law is essential to effective contract management.

The rules change often, and these changes frequently require changes in compliance and contract management practices.

In our view, it is nearly impossible for any contract manager to personally track *all* the individual developments of government contracts and still perform his or her actual job of managing contracts. Fortunately, no contract manager has to. One of the most valuable services that professional associations such as NCMA provides is periodic and year-end analysis of important changes through publications and seminars. In addition, law firms and government contract consultants keep government contractors informed of changes and prospective changes through advisories and seminars, most of which are free and open to the public. In short, contract managers can sign up and receive valuable information from a variety of sources.

In addition to keeping informed, contract managers must be sure to address changes in their internal compliance programs and contract management procedures. At least yearly, contract managers should meet with their compliance and legal departments to assess the annual changes and revise internal policies accordingly. While perhaps not the most festive of year-end or year-beginning practices, it is a vitally important one. CM

CONTRIBUTED BY THE GOVERNMENT CONTRACTS PRACTICE GROUP AT DRINKER BIDDLE & REATH LLP.

- drinkerbiddle.com
- twitter.com/DrinkerBiddle
- linkedin.com/company/drinker-biddle-reath
- facebook.com/DrinkerBiddleReathLLP

ENDNOTES

1. We limit our discussion to statutory, regulatory, and new (i.e., became effective in 2019) changes, thus excluding proposed changes that are still under consideration (including proposed *FAR* and *FAR* supplement rules that are in the comment period).
2. *Available at* https://www.justice.gov/jm/jm-4-4000-commercial-litigation#4-4.112.
3. 31 USC 3729–3733.
4. I.e., Section 4-4.112, "Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters."
5. *See* DOJ, "Evaluation of Corporate Compliance Programs" (April 2019), *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.
6. 31 USC 3731(b).
7. *Cochise Consultancy Inc., v. United States ex rel. Hunt,* No. 18-315 (U.S. May 13, 2019).
8. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.,* No. 15-cv-2245, 2019 WL 2024595 (E.D. Ca. May 8, 2019).
9. *Universal Health Services., Inc. v. United States ex rel. Escobar,* 136 S. Ct. 1989, 2001 (2016).
10. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., op. cit.*
11. *Ibid.*
12. *Ibid.* (emphasis added).
13. *Ibid.*
14. *Ibid.*
15. No. 1:11-cv-00400-RJA (W.D.N.Y.).
16. Ellen Lord, Under Secretary of Defense (Acquisition and Sustainment), "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review" (January 21, 2019), *available at* https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.
17. *Ibid.*
18. *Ibid.*
19. For more information, see https://www.acq.osd.mil/cmmc/index.html.
20. *Ibid.*
21. *Ibid.*
22. NIST SP 800-171 Rev. 2, *available at* https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-2/draft/documents/sp800-171r2-draft-ipd.pdf.
23. NIST SP 800-171B, *available at* https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf.
24. *See* NIST SP 800-171B, *ibid.*
25. NIST, "Request for Comments on Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations—Enhanced Security Requirements for Critical Programs and High Value Assets," *available at* https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf.
26. *Pub. L.* 114-328.
27. 42 USC 5122.
28. *Pub. L.* 115-91.
29. *Pub. L.* 115-232.
30. James Geurts, Assistant Secretary of the Navy (Research, Development, and Acquisition), "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks" (September 28, 2018), *available at* https://www.insidegovernmentcontracts.com/wp-content/uploads/sites/11/2019/09/ASN-SIGNED-IMPLEMENTATION-OF-ENHANCED-SECURITY-CONTROL.pdf.
31. DOD, "Summary of the 2018 Department Of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity" (February 12, 2019), *available at* https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
32. *Ibid.,* at 4.
33. *Ibid.,* at 7–8.
34. *Ibid.,* at 9.
35. NIST, "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools" (April 9, 2019), *available at* https://www.nist.gov/sites/default/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.
36. Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence" (February 11, 2019), *available at* https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.
37. NIST, "U.S. Leadership in AI," *op. cit.,* at 3.
38. *Ibid.*
39. *Ibid.,* at 4.
40. *Ibid.*
41. *Ibid.*
42. *Ibid.,* at 4–6.
43. DFARS Case 2017-D014.
44. DFARS Case 2017-D040.
45. DFARS Case 2018-D016.
46. *Pub. L.* 114-92.
47. FAR Case 2017-006.
48. DFARS Case 2017-D009.
49. *See* note 47.
50. DFARS Case 2018-D008.
51. DFARS Case 2018-D072.
52. *Ibid.*
53. Executive Order 13881, "Executive Order on Maximizing Use of American-Made Goods, Products, and Materials" (July 15, 2019), *available at* https://www.whitehouse.gov/presidential-actions/executive-order-maximizing-use-american-made-goods-products-materials/.
54. 41 USC Chapter 83 (formerly the "Buy American Act").
55. *Alutiiq Manufacturing Contractors, LLC v. United States,* Civ No. 15-881C (Ct. Fed. Cl. June 27, 2019).
56. *Ibid.*
57. *Lisbon Contractors, Inc., v. United States,* 828 F.2d 759 (Fed. Cir. 1997).
58. *Alutiiq* (*see* note 55), *citing Lisbon* (*ibid.*).
59. *Food Marketing Institute v. Argus Leader Media,* No. 18-481 (U.S. June 24, 2019).
60. 5 USC 552.
61. *National Parks & Conservation Assn. v. Morton,* 498 F.2d 765 (D.C. Cir. 1974).
62. *Ibid.*