

THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement



Vol. 59, No. 22

June 14, 2017

Focus

In this issue ...

FOCUS

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 4—Subcontracts, Joint Ventures And Teaming Agreements ¶ 177
♦By John Chierichella, Townsend Bourne and Melinda Biancuzzo.

DEVELOPMENTS

DOD, EPA Need To Improve SBIR Spending Data Reporting ¶ 178

GAO Testifies On Coast Guard Acquisition Budget Concerns ¶ 179

Developments In Brief ... ¶ 180

DECISIONS

Prudential Standing Doctrine Applies To Protests, COFC Holds ¶ 181

Agency's Past Technical Performance Was Flawed, Comp. Gen. Says..... ¶ 182

¶ 177

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 4—Subcontracts, Joint Ventures And Teaming Agreements

Our “Cyber-Fitness” series thus far has focused on a contractor’s individual obligations and best practices for compliance with the Federal Acquisition Regulation and Defense FAR Supplement cybersecurity rules. But cybersecurity is not an insular discipline, disconnected from the relationships that contractors have with third parties. The acts and omissions of third parties can compromise information furnished to them as members of a contractor’s supply chain, and those same third parties can also compromise the contractor’s systems.

Thus, contractors must be mindful of the cybersecurity capabilities of subcontractors, joint-venture partners and teammates. Indeed, some of the most high-profile data breaches in recent years have been linked to data security vulnerabilities in the supply chain and third-party vendors. While it remains to be seen exactly how and in what situations a contractor may be liable for the actions or inactions of other contractors in the cybersecurity realm, contractors would be unwise to assume that third-party cybersecurity issues are not their issues as well.

To the contrary, Department of Defense guidance suggests that contractors will be responsible, at least in some instances, for the noncompliance of their subcontractors and cloud service providers (CSPs). Thus, basic knowledge of the capabilities and vulnerabilities of subcontractors, partners and teammates, as well as an understanding of each party’s cybersecurity obligations under their contracts with each other, are vital. Obtaining that knowledge about suppliers and partners may be more easily said than done, but cybersecurity due diligence should not be ignored.

Focus continued on page 3 ...

◆ Index ◆

Focus

FEATURE COMMENT: Achieving Cyber-Fitness
 In 2017: Part 4—Subcontracts, Joint Ventures
 And Teaming Agreements ¶ 177
 ◆ By John Chierichella, Townsend Bourne and
 Melinda Biancuzzo.

Developments

DOD, EPA Need To Improve SBIR Spending Data
 Reporting ¶ 178

GAO Testifies On Coast Guard Acquisition Budget
 Concerns ¶ 179

Developments In Brief ¶ 180

- (a) DOD IG Substantiates Healthcare Contractor’s
 Whistleblower Retaliation
- (b) CRS Updates Review of Efforts to Develop Unique
 Contractor Identity Numbers
- (c) Canada Threatens to Scrap F-18 Aircraft
 Procurement
- (d) USPS Must Improve Compliance with Labor
 Substitution Policies
- (e) White House Issues Principles for ATC
 Privatization

Decisions

A ◆ has been added at the end of headlines in this section to
 indicate cases having an accompanying analytical note.

Prudential Standing Doctrine Applies To Protests,
 COFC Holds◆ ¶ 181
Cleveland Assets, LLC v. U.S., 2017 WL 2384774
(Fed. Cl. May 22, 2017)

Agency’s Past Technical Performance Was Flawed, Comp.
 Gen. Says ¶ 182
TOTE Servs., Inc., Comp. Gen. Dec. B-414295, et al.,
2017 CPD ¶ 158

— Case Table —

Cleveland Assets, LLC v. U.S., 2017 WL 2384774 (Fed.
 Cl. May 22, 2017) ¶ 181

TOTE Servs., Inc., Comp. Gen. Dec. B-414295, et al.,
2017 CPD ¶ 158 ¶ 182

This installment in our series summarizes the cybersecurity regulatory flow-down requirements, as well as issues relevant to entering into a joint venture or teaming agreement.

Flow-Down Provisions—Both the FAR and DFARS rules include a flow-down requirement. FAR 52.204(c) states,

Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items [COTS]), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

Emphasis added. This is a broad mandate that subcontractors will be subject to the same rules as their prime contractors whenever the subcontractor will handle federal contract information (FCI).

Note that this clause exempts subcontracts for COTS items from the flow-down requirement. This exemption may be more a testament to the efficacy of the COTS lobby than to any other factor.

Query: What justification is there for distinguishing between COTS suppliers and suppliers of FAR pt. 12 “commercial items”? Frankly, a COTS supplier that has FCI “residing in or transiting through its information system” is just as vulnerable to cyber attack as any other contractor, perhaps more so.

If the rationale for this exemption is the assumption that COTS suppliers are not likely to have such information in their systems, the exemption is unnecessary to the extent that the assumption is correct, because the flow-down is required only if FCI resides in or transits through the system. However, if the assumption is not invariably correct, the FAR rule leaves a gaping hole in the supply chain’s cybersecurity defenses.

DFARS 252.204-7012(m) provides as follows:

Subcontracts. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information

required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a [National Institute of Standards and Technology, Special Publication (SP)] 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii) (B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

The DFARS clause requires flow-down if a subcontractor will handle covered defense information (CDI) or if a subcontract is for “operationally critical support” (defined as “supplies or services designated by the government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation”). DOD’s answers to industry questions clarify that the contractor “should” consult with the CO to determine whether the subcontract will involve CDI and will require flow-down of the clause. See DOD FAQs Regarding Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), DFARS subpt. 204.73 and Procedures, Guidance and Information subpt. 204.73, and DFARS subpt. 239.76 and PGI subpt. 239.76, FAQ No. 5 (Jan. 27, 2017), available at [www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_\(01-27-2017\).pdf](http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf).

DOD also clarified that the clause is not required in contracts solely for COTS items, but it did not address specifically the applicability to **subcontracts** involving only COTS items. See DOD FAQs, supra at No. 3; 81 Fed. Reg. 72987 (prescriptions at DFARS 204-7304 for use of DFARS clause exclude COTS contracts). Thus, it is possible the clause would be required to be flowed down to a subcontractor providing only COTS items if the prime contract is not solely for COTS items.

Again, the wisdom of this COTS exemption generally is open to question. Note that DOD will hold an Industry Information Day on June 23 that will include a briefing and will address questions to further clarify the DFARS requirements. See 82 Fed. Reg. 16577 (Apr. 5, 2017).

There may be situations in which both the FAR and DFARS clauses will be included in a solicitation or contract because the effort involves both FCI and CDI. In such cases, a contractor will need to examine its subcontract effort to determine whether both, one or neither of the clauses should be flowed down. See FAQs, No. 7 (“Most solicitations/contracts that include CDI will also include non-CDI Federal contract information ... it is likely that non-CDI Federal contract information will be flowed down to a subcontractor even when CDI is not, and as such, the FAR clause will flow down”).

With regard to CSPs, the DFARS clause is to be flowed down if a CSP will act as a subcontractor. See FAQs, No. 57. Where a CSP will not act as a subcontractor, but will be used “to store, process or transmit any covered defense information for the contract,” it must comply with the Federal Risk and Authorization Management Program (FedRAMP) moderate baseline (per DFARS 252.204-7012(b)(2)(ii)(D)).

Subcontractor Reporting Requirements—

Neither the FAR nor the DFARS clause requires a subcontractor to notify the prime contractor immediately of the occurrence of a cyber incident or of the details surrounding an incident. The DFARS clause requires merely that a subcontractor provide the incident report number associated with a cyber incident to the prime contractor “as soon as practicable” after reporting the incident to DOD.

It is unclear what a prime contractor’s role will be if a subcontractor experiences a cyber incident. Under the existing regulation, the prime may be given essentially no information regarding the breach and, thus, may be concerned that its information was compromised. Further, the prime contractor’s hands will be tied if the Government expects the prime to enforce compliance or respond to a subcontractor incident for which it has inadequate information.

The DFARS clause includes a requirement that the contractor notify DOD within 30 days after contract award of security controls not implemented at the time of award. DFARS 252.204-7012(b)(2)(ii)(A). This

provision is flowed down to subcontractors because the DFARS clause must be flowed down “without alteration.”

However, there is no requirement that the subcontractor notify the prime contractor of any noncompliance. Per subsection (m), a subcontractor must notify the prime contractor (or next higher-tier contractor) only of requests to the CO to vary from NIST SP 800-171 requirements. A subcontractor is not required to provide to the prime contractor the documentation regarding the variance that it provided to the Government. To ensure that prime contractors are not blind to information that could prove to be important to them and to the security of their information, prime contractors and subcontractors should have a clear contractual agreement, notwithstanding the language of DFARS 252.204-7012(m), regarding what information will be shared by the subcontractor, and when it will be shared.

Subcontractor Compliance and Supply Chain Risk—Contractors may have more responsibility than they realize when it comes to subcontractor compliance with cybersecurity requirements. In fact, DOD has suggested that prime contractors will be responsible for ensuring subcontractors’ compliance with the requirements. For example, requirements flowed down “should be enforced by the prime contractor as a result of compliance with these terms.” FAQs, No. 5.

Similarly, as noted above, if a contractor uses a CSP subject to the FedRAMP moderate baseline per DFARS 252.204-7012(b)(2)(ii)(D), “the flow-down provision in 252.204-7012 does not apply ..., [but] the prime contractor is responsible to ensure that the CSP meets the requirements [for the FedRAMP moderate baseline].” See FAQs, No. 57. Thus, it appears DOD will hold contractors accountable for the FedRAMP compliance of their CSPs as well as for subcontractor compliance with other cybersecurity requirements.

Prime contractors and subcontractors should address, prior to contract formation and in their contract documents, any cybersecurity requirements above and beyond those flowed down through the FAR and DFARS clauses. Depending on the arrangement, including the size, experience and reputation for compliance of the supplier, contractors may feel comfortable relying on the existing FAR and DFARS provisions. Smaller, less-experienced suppliers may warrant a more hands-on approach.

It may well be that the market in this respect is highly reactive, i.e., if the Government evidences a propensity to punish contractors for the noncompliance of their subcontractors, an aggressive approach may become standard on the part of prime contractors and higher-tier subcontractors. Examples of additional steps that prime contractors might take to enhance their confidence in subcontractor cybersecurity compliance include:

- certification of compliance with security controls (e.g., NIST SP 800-171) provided through a third-party auditor or through self-certification,
- reports by a subcontractor to the prime contractor regarding a cyber incident within a defined time frame,
- cybersecurity insurance—to provide protection against cyber incident losses and to cover third-party claims, and
- a subcontractor indemnity.

The above examples obviously are not an exhaustive list of the mechanisms available to increase a prime contractor's confidence in a supplier's cybersecurity compliance, to mitigate the risk of noncompliance, or to demonstrate to the Government the contractor's good faith, reasonable (i.e., not reckless or indifferent) approach to "down the chain" cybersecurity compliance.

In addition to ensuring subcontractor compliance with the FAR and DFARS provisions, prime contractors have an obligation in some instances to mitigate supply chain risk in the provision of supplies and services to the Government. DFARS 252.239-7018, Supply Chain Risk, is to be included in all contracts for information technology involving a national security system. See DFARS 239.7306. Supply chain risk, as used in DFARS 252.239-7018, means "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

The clause is not specific as to the actions a prime contractor must take to mitigate supply chain risk, but, if a contractor flows down all of the cybersecurity requirements pursuant to FAR 52.204-21 and DFARS 252.204-7012, it is unclear what more

reasonably could be expected in this regard (where the FAR clause mandates implementation of 15 security controls in NIST SP 800-171 and the DFARS clause requires compliance with all NIST SP 800-171 controls).

Beyond the FAR and DFARS flow-down requirements, which are extensive, contractors may wish to refer to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations. This publication includes an overlay of supply chain risk management controls that may be implemented in conjunction with the security control families in NIST SP 800-53 and, by extension, NIST SP 800-171.

Providing further incentive for contractors to address supply chain risk is the president's recent executive order on cybersecurity, which includes a provision focusing on review of the supply chain for the defense industrial base, suggesting this area is likely to be more highly scrutinized in the near future. See Executive Order 13800.

Considerations for Joint Venture or Teaming Agreements—Before entering into a joint venture or teaming agreement, contractors should consider the cyber-fitness of any potential partner to assess risk, assess the value of the prospective business relationship, and facilitate more productive negotiations. Many companies, understandably, will resist any meaningful review on the cybersecurity front on the theory that it will involve an unwarranted and unnecessary intrusion into a proprietary domain. The larger the partner, the more likely this resistance will be encountered. Many contractors will take the position that flow-down requirements, certificates of compliance or indemnities are adequate protection for the other members of the business relationship.

Where the parties are amenable to sharing information regarding their cybersecurity capabilities, they may wish to review jointly the means by which each party complies or plans to comply with the applicable security controls in NIST SP 800-171. This could include discussion regarding data storage and security, as well as policies and procedures for data recovery and reporting. Such collaboration may improve the cybersecurity capabilities of both contractors if new methods for achieving cyber-fitness are shared.

Conclusion—Companies inhabit an interdependent and interactive world, and with that

interaction comes risk. That risk is no more challenging than in the area of cybersecurity in which the technology evolves rapidly and the ingenuity of the malefactors seems to expand exponentially. The FAR and DFARS impose a variety of cybersecurity and supply chain security requirements on prime contractors and subcontractors, and it appears that DOD will expect contractors to oversee and enforce subcontractor compliance with these requirements.

With the scope of a contractor's liability for supply chain risks uncertain at this juncture, vigilance, diligence and attention should be the watchwords of the day. It may not be enough simply to rely on a boilerplate form that flows down the FAR and DFARS clauses, and assume that you have met your obligation or that you have adequately mitigated your risks.



This Feature Comment was written for THE GOVERNMENT CONTRACTOR by John Chierichella, Townsend Bourne and Melinda Biancuzzo. Mr. Chierichella is a partner in the Washington, D.C. office of Sheppard, Mullin, Richter & Hampton, a member of the firm's Government Contracts, Investigations, and International Trade practice group, and co-leader of the firm's Aerospace and Defense Industry team. Ms. Bourne and Ms. Biancuzzo are associates in Sheppard Mullin's Washington, D.C. office and members of the Government Contracts, Investigations, and International Trade practice group. They can be reached at jchierichella@sheppardmullin.com, tbourne@sheppardmullin.com and mbiancuzzo@sheppardmullin.com, respectively.

Developments

¶ 178

DOD, EPA Need to Improve SBIR Spending Data Reporting

Most agencies met spending requirements for their Small Business Innovation Research (SBIR)

and Small Business Technology Transfer (STTR) programs in fiscal year 2015, but the Department of Defense and Environmental Protection Agency failed to collect and submit data on their extramural research and development obligations to calculate required spending levels, the Government Accountability Office has reported.

In the SBIR and STTR programs, agencies award contracts and grants “to support the development and commercialization of innovative technologies,” GAO explained. The Small Business Act requires agencies to make SBIR and STTR awards worth specified percentages of their extramural R&D obligations. “Extramural R&D is generally conducted by nonfederal employees outside of federal facilities,” GAO said.

R&D Data Reporting—Nine of the 11 agencies with SBIR programs submitted data on extramural R&D obligations to the Small Business Administration, and four of the five agencies with STTR programs did so. However, GAO found that DOD and EPA “do not have procedures for collecting the data, and they face challenges in collecting these data.”

In FY 2015, agencies were required to spend at least 2.9 percent of extramural R&D obligations in SBIR programs and 0.4 percent in STTR programs. Eight of the nine agencies that submitted data met the SBIR spending threshold, GAO reported. The Department of Agriculture missed the requirement, spending 2.5 percent of its extramural R&D obligations on SBIR awards. All four STTR agencies that submitted data met the STTR spending threshold.

SBA has not submitted its annual SBIR and STTR report to Congress for FY 2014 or FY 2015, GAO admonished. SBA is still working to implement a prior GAO recommendation to submit timely annual reports. See 55 GC ¶ 288. SBA officials noted that “it is difficult to predict the completion of an Office of Management and Budget review” that is not in the SBA's control.

Calculating Spending Requirements—Officials at most of the agencies reported difficulties in calculating spending requirements using extramural R&D obligations data. GAO noted its finding in 2016 that some agencies “believe it is unfair or impractical to hold their agencies to a requirement based on obligations, which are not known until after the end of the fiscal year, when it is not pos-

sible to obligate additional money for the SBIR and STTR programs.” See 58 GC ¶ 211.

An interagency working group is considering recommendations for an alternative spending calculation, such as basing requirements on extramural R&D budget authority, GAO noted. “If Congress were to take up such a proposal, it might eliminate the data collection challenges that some agencies have identified.” GAO determined that basing the spending requirements on total R&D budget authority, instead of extramural R&D obligations, would have increased SBIR and STTR spending from \$2.5 billion to \$4.4 billion in FY 2015.

GAO flagged inconsistencies in how agencies reported calculating their SBIR and STTR spending requirements. For example, not all agencies itemized exclusions or fully explained the reasons for exclusions. Further, only five of the agencies timely submitted their methodology reports.

GAO could not determine SBIR and STTR administrative costs because agencies are not required to track such costs. Nine agencies participating in a pilot program reported \$33.9 million in SBIR and STTR administrative costs in FY 2015. However, the figure does not represent their total administrative spending.

Recommendation—GAO recommended that DOD and EPA develop procedures to report extramural R&D obligations data or propose an alternative methodology to calculate their spending requirements.

Under the Small Business Act, agencies with extramural R&D obligations of \$100 million or more must operate a SBIR program, and those with \$1 billion or more must operate a STTR program. Other agencies with a SBIR program are NASA, the National Science Foundation, and the departments of Commerce, Education, Energy, Health and Human Services, Homeland Security, and Transportation. DOD, DOE, HHS, NASA and NSF also have STTR programs.

In May, GAO and SBA officials testified on SBIR and STTR reform before two House subcommittees, and GAO reported that not all agencies have implemented SBIR and STTR antifraud controls, as required. See 59 GC ¶ 127; 59 GC ¶ 136.

Small Business Research Programs: Most Agencies Met Spending Requirements, but DOD and EPA Need to Improve Data Reporting

(GAO-17-453) is available at www.gao.gov/assets/690/684990.pdf.

¶ 179

GAO Testifies On Coast Guard Acquisition Budget Concerns

New Coast Guard acquisitions have lost operational days because of problems with critical equipment, and there remains a funding gap “between the funding amounts the Coast Guard estimates its major acquisitions need and what it has requested,” Marie Mak, director of acquisition and sourcing management at the Government Accountability Office, testified June 7 before the House Transportation and Infrastructure Subcommittee on Coast Guard and Maritime Transportation.

According to Mak, the Coast Guard is currently procuring three new cutter classes—the National Security Cutter (NSC), the Offshore Patrol Cutter (OPC), and the Fast Response Cutter (FRC)—“that are intended to have more capability than the legacy assets they are replacing,” but the FRC and NSC in particular have been “plagued by problems with critical equipment, such as the diesel engines, which have contributed to lost operational days.” In March, GAO reported that although both the FRC and the NSC “met their minimum mission capable targets on average over the long-term, more recently—from October 2015 to September 2016—they fell below their minimum targets due to needed increased depot-level maintenance.” See 59 GC ¶ 102(c).

Mak pointed out that “the NSC’s engines overheat in waters above 74 degrees, which makes up a significant portion of the NSC’s operating area given that they are intended to be deployed worldwide,” and the FRC fleet has required 20 engine replacements. Although the cost of the FRC engine replacements was covered by contract warranty, GAO has “consistently reported concerns about the affordability of the Coast Guard’s acquisition portfolio,” Mak continued. “While the Coast Guard is in the process of developing a long-term acquisition strategy, it continues to use its annual budget request as its primary strategic planning tool to manage its major acquisitions.”

“In an effort to address funding constraints, the Coast Guard delayed new acquisitions through the annual budget process, but lacks a long-term plan to set forth affordable priorities,” Mak added. “As a result of these issues, it is facing a gap in the capability provided by its Medium Endurance Cutters, which are slated to reach the end of their service lives before all the OPCs are operational.”

“Since 2014, [GAO has] found that there are funding gaps between what the Coast Guard estimates it needs and what it traditionally requests and receives,” Mak testified. “The affordability of the Coast Guard’s portfolio will only worsen once it starts funding the [OPC].” GAO testified before the same subcommittee in 2015 that the Coast Guard’s “needs outpace available funds,” despite progress improving its acquisition management capabilities. See 57 GC ¶ 164. “This has continued,” Mak said. “For example, senior Coast Guard officials peg acquisition needs at over \$2 billion per year, but the President’s budget requested \$1.2 billion for fiscal year 2018.”

Mak cautioned that the Coast Guard’s budget “does not reflect realities. For example, if you look at the president’s 2018 budget request, the OPCs cost almost half a billion [dollars], almost half of the acquisition budget.” Mak continued, “The FRCs [cost] almost a quarter of the acquisition budget, so that leaves you a quarter left that does not address the 10 NSCs, the FRC plus-ups, the icebreakers, the service life extension for the medium endurance cutters or the shore infrastructure which we’ve already said is \$1.6 billion in terms of backlog.”

According to Mak, “GAO recommended in 2014 that the Coast Guard develop a 20-year fleet modernization plan that identifies all acquisitions needed to maintain the current level of service ... and the fiscal resources needed to buy the identified assets.” Although the Department of Homeland Security concurred with GAO’s recommendation, “it is unclear when the Coast Guard will complete this effort,” Mak observed. “Efforts are underway to address this issue through the development of a 20-year capital investment plan ... but to date efforts by DHS and the Coast Guard have not led to the difficult tradeoff decisions needed to begin addressing the long-term affordability of its portfolio.”

¶ 180

Developments In Brief ...

- (a) **DOD IG Substantiates Healthcare Contractor’s Whistleblower Retaliation**—Department of Defense contractor Bio-Medical Personnel Services Inc. (BPSI) retaliated against two employees for making protected disclosures about tasks outside the scope of a task order and a lack of proper equipment, the DOD inspector general reported June 6. In 2009, the Army National Guard awarded BPSI a contract for professional and administrative support services. In 2015, a BPSI multimedia specialist and a multimedia photographer filed DOD hotline reports alleging that they had been assigned tasks unrelated to the production of a half-hour television program, the focus of the task order, and that they had not been provided with proper equipment. After the complaints were initially dismissed, Sens. Claire McCaskill (D-Mo.) and Charles Grassley (R-Iowa) expressed concern that the IG may have misinterpreted the relevant statute. On reconsideration, the IG determined that the employees reported information to the Missouri National Guard Joint Force Headquarters IG with a reasonable belief in an abuse of authority, making their reports protected disclosures. BPSI placed the employees on administrative leave and later discharged them, which the DOD IG substantiated as reprisal in violation of 10 USCA § 2409. The IG noted that BPSI apparently dissolved in 2015. The IG recommended that the National Guard Bureau (a) consider appropriate action against BPSI or any successor in interest and (b) order BPSI or any successor to reinstate the employees, expunge the personnel action from their records, and award them compensatory damages and back pay. Lawmakers have taken the DOD IG to task for its narrow interpretation of the officials to whom whistleblowers may make protected disclosures. See 56 GC ¶ 331. Section 827 of the National Defense Authorization Act for Fiscal Year 2013 expanded whistleblower protections for contractor employees under § 2409. See Schaengold and Deschauer, Feature Comment, “The Impact Of The FY 2013 NDAA On Federal Procurement,” 55 GC ¶ 57. The IG’s

reports (DODIG-2017-083, DODIG-2017-088) are available at www.dodig.mil/pubs/documents/DODIG-2017-083.pdf and www.dodig.mil/pubs/documents/DODIG-2017-088.pdf.

(b) CRS Updates Review of Efforts to Develop Unique Contractor Identity Numbers—

The Congressional Research Service recently provided an updated look at the Government's efforts to replace Dun and Bradstreet Inc.'s (D&B's) proprietary Data Universal Numbering System (DUNS), which provides federal contractors with unique identifying numbers. In 2016, CRS surveyed efforts by the General Services Administration, the Office of Management and Budget, and the Treasury Department to develop possible alternatives to replace DUNS numbers with a new system. See 58 GC ¶ 174(c). DUNS numbers and other services the Government obtains from D&B are "integral to the functioning of various procurement processes and activities," CRS observed. However, the numbers are proprietary, with restrictions on how they can be used. In 2012, the Government Accountability Office highlighted the higher costs of using the system, and "examined possible alternatives to DUNS and anticipated challenges in replacing DUNS with a different identification system." See 54 GC ¶ 191. "In early 2017, GSA initiated a process for exploring alternatives to DUNS by posting a request for information (RFI) for entity identification and validation services on the Federal Business Opportunities (FedBizOpps) website," CRS noted. The RFI said the Government "is exploring all viable means of continuing to meet its ongoing need for entity identification and validation services." In May, GSA noted that "it had received 'an impressive number and variety of responses' from industry and other stakeholders and that it had begun reviewing the responses 'to determine the viability of proposed alternatives,'" CRS added. "GSA's tentative schedule is to issue a solicitation in summer 2017 and award a contract prior to the expiration of its contract with [D&B], which will occur in June 2018." *Unique Identification Codes for Federal Contractors: DUNS Numbers and CAGE Codes* is available at fas.org/sgp/crs/misc/R44490.pdf.

(c) Canada Threatens to Scrap F-18 Aircraft Procurement—

The Canadian government "is disappointed in the action of one of our leading industry partners," Canadian Minister of National Defence Harjit Sajjan said in a recent address to members of the Canadian armed forces. "We strongly disagree with the decision of the United States Commerce Department to initiate a trade remedy case in response to Boeing's petition against Bombardier." In April, Commerce and the U.S. International Trade Commission opened an investigation into Boeing Co.'s complaint that Bombardier Inc. violated antidumping rules and received unfair Canadian subsidies for 100- to 150-seat large civil aircraft. Sajjan added, "Canada is reviewing our procurement involving that firm." Canada is considering a proposed procurement of 18 Boeing F-18 Super Hornet fighters as part of an interim fleet until it can fully replace its aging fleet. "The interim fleet procurement requires a trusted industry partner," Sajjan said. "However, our government is of the view that [Boeing's] action against Bombardier is unfounded ... and we call on Boeing to withdraw it." Sajjan also called on "all of our industry partners to speak with one voice about the interconnectedness of the defence-industry supply chains in Canada and the United States." The Trump administration recently imposed a new tariff on Canadian lumber and has called for renegotiation of the North American Free Trade Agreement. "We need your help making the clear case for ensuring goods continue to flow freely between our two countries," Sajjan told Canada's industry partners. "We need your voices to articulate the consequences should our borders be closed." Boeing's complaint was docketed as number 3219 with the investigation numbers 701-TA-578 and 731-TA-1368.

(d) USPS Must Improve Compliance with Labor Substitution Policies—

Contracting officers did not comply with the U.S. Postal Service's policy for labor substitution of key personnel on goods and services contracts, the USPS inspector general recently reported. In 89 of 187 invoices reviewed from fiscal years 2015 and 2016, the IG identified contract personnel who were substituted as key personnel without written approval. The IG concluded this occurred because of "poor CO contract oversight and inadequate documentation practices in managing key per-

sonnel.” Without written approval, USPS cannot substantiate the substitution of key personnel with individuals of “like experience and qualifications.” The IG found that this increases the risk of substandard service, project delays and cost overruns. The IG recommended USPS reiterate existing policy on key personnel clauses, contract documentation practices and use of the Contract Authoring and Management System. The IG also recommended that USPS establish an oversight process to ensure proper review, approval and documentation of labor substitution for key personnel. *U.S. Postal Service Contract Labor Substitution* (SM-AR-17-005) is available at www.uspsoig.gov/sites/default/files/document-library-files/2017/SM-AR-17-005.pdf.

- (e) **White House Issues Principles for ATC Privatization**—Asserting that the Federal Aviation Administration’s current air traffic control (ATC) operations are “mired within a Federal bureaucracy that hinders innovative operations and the timely introduction of new technology,” the Trump Administration June 5 released the president’s principles for reforming the U.S. ATC system. The principles include safety; national security; cybersecurity; open access to all users, including rural communities and the military; and the creation of a new nonprofit entity to oversee ATC operations. Another principle is noise, for which “[t]he new ATC entity must have the authority, after seeking public comment, to adjust airspace routes,” according to the administration. “The proposed route change would only be subject to National Environmental Policy Act (NEPA) review if the change exceeds the FAA-established noise threshold.” The transition from FAA to the new entity should be completed within a three-year transition period, the administration said. The ATC entity should be fully financed through user fees and should have the authority to borrow and enter into contracts and leases within the transition period. All ATC assets currently owned by FAA should be transferred to the new entity “at no charge,” along with sufficient funds to account for environmental liabilities associated with such assets. For the entity’s board of directors, several stakeholders would

provide lists of qualified candidates, with the secretary of transportation selecting two board members each from the lists provided by the Department of Transportation, major U.S. airlines and employee unions, and one member each from the lists provided by groups representing general aviation and airports. Additional members would be chosen by members selected by the transportation secretary. Transferring ATC operations to a new entity “will enable ATC to keep pace with the accelerating rate of change in the aviation industry, including the integration of new entrants such as Unmanned Aircraft Systems and Commercial Space Transports,” the administration said. In May, the president unveiled his proposed fiscal year 2018 budget, which proposed a nonprofit corporation to assume FAA’s ATC functions. See 59 GC ¶ 171. The administration’s principles are available at www.whitehouse.gov/the-press-office/2017/06/05/president-donald-j-trumps-principles-reforming-us-air-traffic-control.

Decisions

¶ 181

Prudential Standing Doctrine Applies To Protests, COFC Holds

Cleveland Assets, LLC v. U.S., 2017 WL 2384774 (Fed. Cl. May 22, 2017)

The prudential standing doctrine applies to bid protest jurisdiction under 28 USCA § 1491(b). The protester was not within the zone of interest protected by the statute underlying the protest, and the protester therefore lacked standing to assert that protest ground, the U.S. Court of Federal Claims has held. The COFC also held that a \$26 per-square-foot cap on rent did not unduly restrict competition.

The General Services Administration issued a request for lease proposals (RLP) for the Federal Bureau of Investigation field office in Cleveland. The FBI currently leases space from Cleveland Assets LLC, the protester.

For leases with annual rent above \$2.85 million, 40 USCA § 3307(a) provides that “appropriations may be made only if the Committee on Environment and Public Works of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives adopt resolutions approving the purpose for which the appropriation is made.” Section 3307(b) requires GSA to provide Congress with a prospectus describing the rental space and estimating the maximum lease cost.

Several documents in the record analyzed the real estate market and showed rents ranging from \$17.50 to \$50.47 per square foot. The record also included an “Analysis of Replacement Lease Rental Rate” reflecting GSA’s discussions with the Office of Management and Budget that underlie the rental rate listed in the prospectus. That analysis proposed an annual rent of \$3.75 million and estimated a \$26 per-square-foot rental rate.

In 2011, the congressional committees approved a prospectus with a \$26 per-square-foot estimated rate. GSA issued the RLP in December 2016, seeking a 20-year term for 108,850 to 114,290 square feet of office space.

The RLP sought “a fully serviced, turnkey Lease with rent that covers all lessor costs.” The RLP also stated that it was “subject to an approved Prospectus issued in accordance with 40 USC § 3307” and the \$26 per-square-foot rate approved by Congress. The RLP listed the evaluation factors and stated that the lease would be awarded to “the responsible Offeror whose offer will be most advantageous to the Government.”

Standing—Under 28 USCA § 1491(b)(1), the COFC has jurisdiction over an “action by an interested party objecting to a solicitation by a Federal agency for bids or proposals for a proposed contract or to a proposed award or the award of a contract or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement.”

To have standing, a protester must be an “interested party”: an actual or prospective offeror who possesses a direct economic interest in the procurement. *Sys. Application & Techs., Inc. v. U.S.*, 691 F.3d 1374 (Fed. Cir. 2012); 54 GC ¶ 308. An offeror has a direct economic interest if it suffered a competitive injury or prejudice as a result of an alleged error in the procurement process. *Myers Investigative & Sec. Servs., Inc. v. U.S.*, 275 F.3d 1366 (Fed. Cir. 2002); 44

GC ¶ 25. In a pre-award protest, like this one, the focus is on whether the protester demonstrated a non-trivial competitive injury that can be addressed by judicial relief. See *Weeks Marine, Inc. v. U.S.*, 575 F.3d 1352 (Fed. Cir. 2009); 51 GC ¶ 303.

Improper Communications: Cleveland Assets alleged that GSA had selective communications with prospective offerors in violation of General Services Acquisition Regulation 570.302(c) and 570.303-4(a). The communication occurred when Cleveland Assets asked about a discrepancy between the RLP requirement for an automobile annex and other RLP provisions that did not include space for the annex. Cleveland Assets complained that although GSA advised Cleveland Assets not to include an annex in its proposal, GSA did not amend the RLP to reflect this clarification.

This claim alleged a competitive injury, but it was an injury to other offerors, not to Cleveland Assets, the party that received GSA’s clarification. Cleveland Assets therefore lacked standing to bring a claim based on this communication, the COFC said.

Cleveland Assets cited other exchanges between GSA and prospective offerors that “demonstrate the ambiguities in the RLP and the clear benefit all offerors would have gained from the clarifications provided to [other offerors] during these exchanges.” But Cleveland Assets never asserted that these exchanges undermined its competitive position. Therefore it was not an interested party for these claims and lacked standing to assert them.

Violation of 40 USCA § 3307: Cleveland Assets alleged that the RLP exceeded GSA’s leasing authority under 40 USCA § 3307 because the RLP solicited proposals for a lease that included space and structures not identified in the prospectus.

Standing involves constitutional and prudential limitations. *Bennett v. Spear*, 520 U.S. 154 (1997). The Constitution requires that the plaintiff demonstrate an “injury in fact” that is “fairly traceable” to the defendant’s action, and which will likely be redressed by a favorable decision. This requirement is satisfied under § 1491(b) if a protester is an interested party, the COFC said.

In addition, *Bennett* explained that prudential principles also apply to standing. These judicially imposed limits are based on the proper role of the courts. Among them is the requirement that “a plaintiff’s grievance must arguably fall within

the zone of interests protected or regulated by the statutory provision or constitutional guarantee invoked in the suit.” Prudential standing principles apply unless they are expressly negated by statute.

Applying these rules and the reasoning in *Bennett*, the COFC first determined whether 28 USCA § 1491(b) expressly negated the zone-of-interests requirement for any violation of a statute or regulation that occurs in connection with a procurement.

Bennett involved the “citizen suit” provision of the Endangered Species Act (ESA), 16 USCA § 1540(g), which states that “any person may commence a civil suit” to enforce certain ESA provisions. *Bennett* held that the citizen-suit provision expressly “negate[d] the zone-of-interests test (or, perhaps more accurately, expand[ed] the zone of interests).” First, the language used in the citizen-suit provision was “an authorization of remarkable breadth” compared to language Congress ordinarily uses. Second, the Court said that its “readiness to take the term ‘any person’ at face value” was supported by two considerations: (1) the subject matter of the legislation “is the environment (a matter in which it is common to think all persons have an interest),” and (2) the obvious purpose of the provision “is to encourage enforcement by so called ‘private attorneys general.’”

In contrast, § 1491(b) lacks indicia of congressional intent to expressly negate the prudential standing doctrine in bid protests. Unlike the ESA, which authorizes a “citizen suit” by “any person,” the Tucker Act permits bid protests by an “interested party”: an actual or prospective bidder possessing a direct economic interest in the procurement.

The “interested party” standard more closely resembles restrictive formulations in other environmental statutes, which *Bennett* suggested would be subject to prudential standing requirements. See Clean Water Act, 33 USCA § 1365(g) (“a person ... having an interest which is or may be adversely affected”); Energy Supply and Environmental Coordination Act, 15 USCA § 797(b)(5) (“[a]ny person suffering legal wrong because of any act or practice arising out of any violation of subsection (a) of this section”); and Ocean Thermal Energy Conversion Act, 42 USCA § 9124(a) (“any person having a valid legal interest which is or may be adversely affected”).

Unlike the broad group of persons interested in the ESA’s subject matter, parties with a direct interest in the Government’s procurement process

are a narrow group: offerors with an economic interest in the outcome of the procurement. Following *Hallmark-Phoenix 3, LLC v. U.S.*, 99 Fed. Cl. 65 (2011), the COFC held that § 1491 is not intended to create “private attorneys general” to enforce laws of broad application, and § 1491(b) did not negate the prudential standing doctrine.

After concluding that prudential standing applied, the COFC addressed the zone-of-interests test and held that Cleveland Assets’ claim did not fall within the zone of interests protected by § 3307(a). That provision requires congressional approval for high-value leases. Its purpose is to allow Congress to oversee rent expenditures. The statute does not mention private parties or Government contractors, or confer a right to judicial review, the COFC said in dismissing Cleveland Assets’ § 3307 challenge.

Challenge to Rental Cap: Counts III and IV alleged that the \$26 per-square-foot rental cap was unreasonably low, unduly restricted competition, and “improperly shifts all risk to the contractor,” thereby “effectively delet[ing] the technical evaluation factors.” Cleveland Assets further alleged that no lessor could comply with the rental cap and also meet the RLP requirements. These claims are sufficient to establish a non-trivial competitive injury, the COFC said in holding that Cleveland Assets is an interested party with standing to bring Counts III and IV.

Restriction on Competition—After addressing standing, the COFC turned to the argument that the \$26 cap unduly restricted competition. The Competition in Contracting Act requires agencies to create specifications designed to achieve full-and-open competition. *CW Gov’t Travel Inc. v. U.S.*, 99 Fed. Cl. 666 (2011); 53 GC ¶ 365. An agency may impose restrictive requirements only as necessary to meet the Government’s minimum needs. *Am. Safety Council, Inc. v. U.S.*, 122 Fed. Cl. 426 (2015). The “agency’s minimum needs,” however, are “within the broad discretion of agency officials.” *Savantage Fin. Servs. Inc. v. U.S.*, 595 F.3d 1282 (Fed. Cir. 2010); 52 GC ¶ 130. Therefore, if a plaintiff challenges a solicitation as unduly restrictive, it must show that the restrictive solicitation term is so plainly unjustified as to lack a rational basis.

In rejecting Cleveland Assets’ challenge, the COFC said that at each stage of the procurement GSA took reasonable steps to determine the rental cap. GSA obtained an appraisal and met

with OMB before submitting the prospectus, and performed site visits and market surveys before issuing the RLP. Several documents in the record support GSA's conclusion that it could secure space for \$26 per square foot, the COFC said. Moreover, the choice of methodologies used to calculate the \$26 cap is within GSA's discretion. See *McConnell Jones Lanier & Murphy LLP v. U.S.*, 128 Fed. Cl. 218 (2016).

Even if GSA's market analysis was imperfect, the COFC would be reluctant to conclude that a \$26 per-square-foot rental cap is "so plainly unjustified as to lack a rational basis." First, an agency may impose price ceilings that maximize contractor risk and minimize Government risk. *American Safety Council*, 122 Fed. Cl. 426. Second, GSA should be able to issue an RLP to test the feasibility of obtaining rental space at the lowest possible rate, the COFC said.

Cleveland Assets' argument that no offeror could comply with the RLP's requirements and still meet the rental cap was speculative. Several building owners responded to the RLP. Moreover, after discussions and final proposal revisions, GSA could assess the risks of the rental cap and exercise its discretion to decide whether those risks are worthwhile.

Finally, GSA had no appropriations to pay a rent above the \$26 cap. Having been unsuccessful in negotiating a new lease with Cleveland Assets, it was not irrational for GSA to solicit offers within the \$26 cap. The COFC therefore rejected Cleveland Assets' argument that the rental cap was unduly restrictive or otherwise irrational.

◆ **Note**—In *Santa Barbara Applied Research, Inc., v. U.S.*, 98 Fed. Cl. 536 (2011); 53 GC ¶ 237, Judge Firestone held that the prudential standing doctrine did not apply to bid protests under § 1491(b):

[T]he court agrees with [the plaintiff] that the concept of "prudential standing" does not apply to bid protests under section 1491(b) (1). Prudential standing is typically applied to challenges under the Administrative Procedure Act ("APA") 5 U.S.C. § 500 *et seq.*, which has more liberal standing criteria than those set in section 1491(b)(1). In [*Am. Fed. of Gov't Employees, AFL-CIO v. U.S.*, 258 F.3d 1294 (Fed. Cir. 2001) (*AFGE*)], the Federal Circuit held that it was rejecting the "less stringent"

standing requirements imposed under the APA in favor of the "interested party" test, based on the definition in CICA. Under *AFGE*, once a party satisfies the more stringent "interested party" test, standing is established.

See also *MORI Assocs. v. U.S.*, 102 Fed. Cl. 503 (2011) (jurisdictional grant over "any alleged violation of statute or regulation" showed intent to expand standing beyond the zone-of-interests test).

In *Cleveland Assets*, Judge Kaplan rejected *Santa Barbara*, noting that it conflicted with *Bennett*, which held that prudential standing requirements apply broadly beyond the APA unless "expressly negated." Judge Kaplan also said that *AFGE* never reached the question of whether a zone-of-interests test would apply because it concluded that the plaintiff in that case was not an interested party.

For a discussion of prudential standing, see Lambiotte, "Jurisdictional Standing & 'Prudential' Standing in Procurement Protests at the U.S. Court of Federal Claims: a Muddled Relationship," Briefing Papers No. 13-3 (February 2013).

¶ 182

Agency's Past Technical Performance Was Flawed, Comp. Gen. Says

TOTE Servs., Inc., Comp. Gen. Dec. B-414295, et al., 2017 CPD ¶ 158

An agency's past technical performance evaluation was flawed where the agency did not adequately document its evaluation, credited offerors for relevant performance without considering quality and credited offerors for positive performance without considering relevance, the U.S. Comptroller General recently determined.

The Navy issued a request for proposals for operation and maintenance on the Sea Based X-Band Radar vessel. The solicitation contemplated a fixed-price contract with reimbursable elements. The best-value award would be based on price and past technical performance evaluation factors. The RFP included four past technical performance elements: operations and manning, lifecycle management, planned maintenance, and management of repairs. These four elements were further divided into 10 sub-elements each.

The RFP provided that the Navy would review past technical performance to evaluate offerors' probability of meeting solicitation requirements. The agency would first evaluate references' relevancy obtained through interviews or the Past Performance Information Retrieval System. Evaluators would then review past performance quality through review of questionnaire responses and the Contractor Performance Assessment Reporting System.

Seven firms submitted offers, including TOTE Services Inc. and U.S. Marine Management Inc. (USMMI). Following final proposal revisions, the Navy rated TOTE's and USMMI's past technical performance as "substantial confidence." The source selection authority reviewed the evaluations and found USMMI's \$32.41 million proposal represented the best value over TOTE's \$39.30 million proposal. The agency awarded the contract to USMMI, and TOTE protested to the Government Accountability Office.

TOTE first argued that the Navy improperly credited USMMI for favorable quality ratings without evaluating the underlying contracts' relevance. TOTE noted that the agency received completed questionnaires, and found some references included ratings on sub-elements for which the offeror had not identified the contract. The Navy received ratings on 17 sub-elements for which the awardee had not identified the contract. The Navy did not perform a relevancy assessment for those questionnaires. But in 20 instances, the Navy did not receive a questionnaire rating for sub-elements—though USMMI had identified the contract for the sub-element. In both cases, the Comp. Gen. noted, the agency credited the orphan relevancy or rating scores in its confidence assessment, despite missing the score's other half.

The Navy asserted that the 17 orphan questionnaires were only considered as further support for the rating USMMI would have received without them. And for the 20 orphan relevancy ratings, the agency relied on the staff's general and direct knowledge.

In reviewing an agency's evaluation, the Comp. Gen. will consider not only whether the agency deviated from the RFP evaluation criteria, but also whether the actual evaluation was unreasonable. *Am. Dev. Corp.*, Comp. Gen. Dec. B-251876.4, 93-2 CPD ¶ 49; 35 GC ¶ 616. The Comp. Gen. found the agency's past technical performance evaluation to be unreasonable. The RFP provided the agency would make both relevancy and quality determinations for the past performance references, and the agency's

overall confidence assessment would be an integrated assessment based on these determinations.

The Comp. Gen. found that the Navy did not make the dual determination that the RFP envisioned. Instead, the Navy credited some questionnaire ratings without considering associated relevance, and conversely credited some relevance determinations without information on the quality of USMMI's performance. The general range of scores and sub-element confidence ratings included all of these scores. The Comp. Gen. determined that the net effect was to distort the Navy's evaluation by adding quality ratings of unknown relevance and relevancy determinations of unknown quality. This conflicted with the RFP's evaluation scheme.

TOTE next argued that the Navy improperly determined that USMMI's submitted prime contract was very relevant under five of the past technical performance sub-elements. USMMI had submitted the contract as supporting past performance under the five sub-elements and included a general discussion on the work performed—but did not explain how the work was relevant.

The Navy conceded that three of the "very relevant" ratings should have been changed to "relevant" but argued the errors were harmless, and that it relied on evaluators' personal knowledge for the other ratings.

Where an agency does not document or retain evaluation materials, it bears the risk that there may not be adequate supporting rationale in the record to find a reasonable basis. *TriCenturion, Inc., et al.*, Comp. Gen. Dec. B-406032, et al., 2012 CPD ¶ 52; 54 GC ¶ 128.

The Comp. Gen. found that the Navy did not sufficiently document its evaluation to determine whether the Navy's conclusions were reasonable. While the Navy asserted that its evaluators relied on personal knowledge of the offered reference contract, this assertion was not supported in the contemporaneous record, nor did it explain the Navy's admission that three of five relevancy determinations were erroneous.

The Comp. Gen. also found the Navy's "personal knowledge" explanation to be inconsistent with the evaluation report, which pointed to USMMI's proposal narrative as the relevancy determination source, without mention of personal knowledge.

Accordingly, the Comp. Gen. sustained the protest.

THE GOVERNMENT CONTRACTOR ADVISORY BOARD

Terry Albertson

Crowell & Moring LLP
Washington, D.C.

John W. Chierichella

Sheppard, Mullin, Richter &
Hampton, LLP
Washington, D.C.

C. Stanley Dees

Middleburg, Va.

Jay DeVecchio

Morrison & Foerster
Washington, D.C.

Agnes Dover

Hogan Lovells US LLP
Washington, D.C.

Richard L. Dunn

Edgewater, Md.

Elizabeth Ferrell

Larkin Ferrell LLP
Washington, D.C.

Gilbert J. Ginsburg

Washington, D.C.

Andrew D. Irwin

Jenner & Block LLP
Washington, D.C.

Steven Kelman

Harvard University
Boston, Mass.

Richard C. Loeb

University of Baltimore
School of Law

Karen L. Manos

Gibson, Dunn & Crutcher LLP
Washington, D.C.

James J. McCullough

Fried, Frank, Harris, Shriver &
Jacobson LLP
Washington, D.C.

David Nadler

Blank Rome LLP
Washington, D.C.

Ralph C. Nash

Washington, D.C.

Stuart B. Nibley

K&L Gates LLP
Washington, D.C.

Neil H. O'Donnell

Rogers Joseph O'Donnell
San Francisco, Calif.

Paul E. Pompeo

Arnold & Porter Kaye
Scholer LLP
Washington, D.C.

Michael J. Schaengold

Greenberg Traurig, LLP
Washington, D.C.

Ella Schiralli

Gemalto
Washington, D.C.

John G. Stafford, Jr.

Husch Blackwell LLP
Washington, D.C.

Steven N. Tomanelli

Steven N. Tomanelli & Associates
Centreville, Va.

Carl L. Vacketta

DLA Piper US LLP
Washington, D.C.

Joseph D. West

Gibson, Dunn & Crutcher LLP
Washington, D.C.

Steven L. Schooner

Christopher R. Yukins

George Washington University
Washington, D.C.



THE GOVERNMENT CONTRACTOR® (ISSN 0017-2596) is issued weekly, except that no issue is published in the weeks containing January 1, Memorial Day, July 4, Labor Day and December 25, or the week after Thanksgiving ♦ 2017 calendar-year subscription includes annual, accredited "Government Contracts Year In Review Conference" ♦ Attorney Editors: William Schieken, Rick Southern, Ken Berke and Joseph Windsor; Manuscript Editors: Lyrica Johnson and Jennifer LeBerre ♦ Published and copyrighted © 2017 by Thomson Reuters, 610 Opperman Drive, PO Box 64526 St. Paul, MN 55164-0526 ♦ www.west.thomson.com/dceditorial ♦ Postage paid at St. Paul, MN. POSTMASTER: Send address changes to THE GOVERNMENT CONTRACTOR, 610 Opperman Drive, PO Box 64526, St. Paul, MN 55164-0526. For subscription information: call 800.221.9428 or write West, Credit Order Processing, 620 Opperman Drive, PO Box 64833, St. Paul, MN 55164-9753 ♦ All correspondence concerning the content of this publication should be addressed to Thomson Reuters, Attention: THE GOVERNMENT CONTRACTOR—Editorial Staff, 1333 H. St., NW, Suite 700, Washington, DC 20005.

THE GOVERNMENT CONTRACTOR® (2017) Thomson Reuters. Reproduction, storage in a retrieval system, or transmission of this publication or any portion of it in any form or by any means, electronic, mechanical, photocopy, xerography, facsimile, recording or otherwise, without the written permission of Thomson Reuters is prohibited. For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA 978.750.8400; fax 978.646.8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax 651.687.7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

Unless otherwise expressly indicated, the content of THE GOVERNMENT CONTRACTOR® should not be ascribed to THE GOVERNMENT CONTRACTOR® Advisory Board or its individual members. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

THE GOVERNMENT CONTRACTOR®

FIRST CLASS

First Class Mail
U.S. POSTAGE
PAID
Twin Cities, MN
Thomson Reuters

published by Thomson Reuters
610 Opperman Drive
P.O. Box 64526
St. Paul, MN 55164-0526

DATED MATERIAL PLEASE DELIVER PROMPTLY

June 2017						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

July 2017						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23 _{/30}	24 _{/31}	25	26	27	28	29

August 2017						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

**Advanced Government
Contract Administration
Workshop**
July 19-20
Hilton Head Island, SC
\$1325

DFARS Workshop
July 19
Hilton Head Island, SC
\$950

**Government Contract
Compliance**
July 18-19
Hilton Head Island, SC
\$1325

**The Masters Institute in
Government Contracting**
July 17-21
Hilton Head Island, SC
\$1995

**Basics of Government
Contracting**
July 17-19
Hilton Head Island, SC
\$1400

FAR Workshop
July 17-18
Hilton Head Island, SC
\$1325

**Government Contract
Purchasing and
Subcontracting**
July 17-18
Hilton Head Island, SC
\$1325

**The Masters Institute in
Government Contract
Intellectual Property**
July 17-19
Hilton Head Island, SC
\$1400

**Concentrated Course in
Government Contracts**
July 17-20
Hilton Head Island, SC
\$1750

**Government Contract
Accounting**
July 17-18
Hilton Head Island, SC
\$1325

**The Masters Institute in
Government Contract
Costs**
July 18-20
Hilton Head Island, SC
\$1825

**A Practical Guide to the
Incurred Cost Submission
(ICS)**
July 17-18
Hilton Head Island, SC
\$1325

For full brochures of the above seminars, contact Federal Publications Seminars at 1365 Corporate Center Curve, Suite 101, Eagan, MN 55123 ♦ Phone 888.494.3696 ♦ www.fedpubseminars.com