THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

THOMSON REUTERS®

Vol. 59, No. 44 December 6, 2017

In this issue ...

Focus

¶ 363

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 6—Potential Liabilities And Putting It All Together

We are just days away from the December 31 deadline for implementation of the security controls in National Institute of Standards and Technology Special Publication (SP) 800-171 pursuant to the provisions of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. It seems like just yesterday we first discussed the clause in Part 1 of the series, "Achieving Cyber-Fitness In 2017: Part 1—Planning For Compliance," 59 GC ¶ 25, in which we examined the DFARS requirements related to safeguarding covered defense information (CDI) and the FAR clause relating to federal contract information (FAR 52.204-21).

Over the course of the year, we examined other laws and regulations regarding data protection and breach response, including those specific to particular agencies, and recommended a comprehensive data-focused approach to maintaining and securing sensitive information. See "Achieving Cyber-Fitness In 2017: Part 2—Looking Beyond The FAR And DFARS—Other Safeguarding And Reporting Requirements," 59 GC ¶ 43. We further reviewed best practices for achieving compliance with data security provisions and the role of third-party auditors during the process, as well as considerations relevant to working with third parties, including subcontractors, teammates and joint venture partners. See "Achieving Cyber-Fitness In 2017: Part 3—Proving Compliance And The Role Of Third-Party Auditors," 59 GC ¶ 87;"Achieving Cyber-Fitness In 2017: Part 4—Subcontracts, Joint Ventures And Teaming Agreements," 59 GC ¶ 177. Finally, we reviewed in detail the cyber incident notification and response requirements of the DFARS clause. See "Achieving Cyber-Fitness

Focus continued on page 3 ...

✦ Index ✦

Focus

Developments

Regulations

Decisions

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

— Case Table —

In 2017: Part 5—Cyber Incident Reporting And Response," 59 GC ¶ 275.

In this final installment of our series, we address developments in the law relating to cybersecurity and the DFARS clause, including what the Department of Defense now is saying regarding compliance, and we explore some of the potential liabilities and consequences associated with noncompliance and breach—and how to avoid them.

System Security Plans and Plans of Action—During its June 23 Industry Day and in subsequent programs, DOD officials clarified that "compliance" with DFARS 252.204-7012 by the December 31 deadline means that a contractor has completed its system security plan (SSP) (required by NIST SP 800-171 Security Control 3.12.4) and plans of action for security controls not yet implemented (required by NIST SP 800-171 Security Control 3.12.2). Plans of action are to describe:

- how and when any unimplemented security requirements will be met;
- how any planned mitigations will be implemented; and
- how and when contractors will correct deficiencies and reduce or eliminate vulnerabilities in the systems.

DOD Guidance on Implementation of DFARS Clause 252.204-7012 (Sept. 21, 2017) at 3, available at *www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf*; see DOD Industry Day Slides at 61, available at *dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940*. There is no submission requirement and no formal mechanism by which DOD plans to check SSPs and plans of action by the deadline (or afterwards, for that matter). Thus, contractors need not worry about turning into a pumpkin at the stroke of midnight on Jan. 1, 2018.

DOD has stated that it is up to the contractor to ensure it has implemented the security controls set forth in NIST SP 800-171 (as well as any other information system security measures deemed necessary by the contractor to provide CDI security). While the fact that Government agents are not likely to be knocking down doors at the start of the year provides some level of comfort, there are potentially serious consequences for contractors that do not have plans in place, or have not fully implemented the required security controls, by January 1—both in terms of getting new work and maintaining work under existing contracts.

Proposals and Source Selection Decisions—As discussed in Part 5 of this series, a contractor's progress toward implementation of the NIST SP 800-171 security controls may be considered in agency evaluation and source selection decisions. Pursuant to NIST SP 800-171, a contractor's SSP and plans of action may be integral to an agency's decision to contract with an organization for use of a nonfederal system to house controlled unclassified information (CUI). DOD Guidance at 4 ("Federal agencies may consider the contractor's system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization, and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization").

Thus, an agency may decide to include solicitation terms that require contractors to include elements of their SSPs in their technical proposals, which then will be evaluated and considered as part of the ultimate source selection decision. DOD provided examples regarding how an agency might use SSPs and plans of action in source selection:

- Requiring that proposals (i) identify any NIST SP 800-171 security requirements not implemented at the time award and (ii) include associated plans of action for implementation;
- Providing in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award; or
- Stating in the solicitation that the contractor's approach to providing adequate security will be evaluated in the source selection process.

See DOD Guidance at 4–5. Thus, a contractor that is further along the path to compliance, or that can demonstrate full implementation of the controls, stands a much lower chance of a negative evaluation in the above-referenced areas, and possibly a better chance of receiving an award. In some cases, a lack of full compliance may render a proposal ineligible for award if such noncompliance represents a failure to meet clear solicitation terms.

If a contractor believes that a security control is not applicable, or an alternative control can satisfy the requirement, it can raise the issue with

DOD for a formal decision, which DOD says can be made "typically within five business days." DFARS 252.204-7008. DOD explained,

> [T]he offeror must provide a written explanation in their proposal describing the reasons why a security requirement is not applicable, or how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement. The contracting officer will refer the proposed variance to the DoD [chief information officer] for adjudication. The DoD CIO is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures. If the DoD CIO needs additional information, a request is made to the contracting officer. Responses are then returned to the contracting officer who, in turn, advises the contractor of the decision. The timeframe for response by the DoD CIO is typically within five business days. The basis for determining if an alternative to a security requirement is acceptable is whether the alternative is equally effective; the basis for determining a security requirement is "not applicable" is whether the basis or condition for the requirement is absent. While the scope of this rule does not provide for the CIO evaluation to impact the award decision, there is nothing that precludes an activity from drafting the solicitation to provide for this.

81 Fed. Reg. 72986, 72990; see DOD FAQs Nos. 18–20 (available at *dodprocurementtoolbox.com/faqs/cybersecurity*). Thus, the clause contemplates some relief for contractors in situations where the full array of NIST SP 800-171 security controls may be overly onerous, but the process that ensues—*after* proposals are due—seems to ensure that a contractor might well be labeled a "problem child." If an agency seeks the path of least resistance, the "problem child" can easily be determined to be less capable than offerors that promise to provide security in accordance with the stated controls. At a minimum, an awardee offering a "less-capable" set of security controls would make an inviting target for disappointed competitors offering "full compliance." Thus, it may be best for contractors to view this option as a last resort reserved for requirements that clearly are not applicable or can be alternatively satisfied. DFARS 252.204-7012(b)(2)(ii)(B) provides a process by which a contractor may request a variance from the DOD CIO if circumstances change after award. See DOD FAQs No. 19.

Bid Protests—So far, the Government Accountability Office has largely stayed out of cybersecurity disputes and allowed agencies to determine what level of security is adequate at the evaluation stage. Last year, GAO denied two protests in which disappointed offerors asserted that an awardee should not have been awarded a contract because it lacked sufficient cybersecurity capabilities. *Discover Techs. LLC*, Comp. Gen. Dec. B-412773 et al., 2016 CPD ¶ 142; 58 GC ¶ 207; *Booz Allen Hamilton, Inc.*, Comp. Gen. Dec. B-412744 et al., 2016 CPD ¶ 151 (note these decisions do not relate specifically to compliance under the DFARS provisions for safeguarding information, but are informative for the way in which they treat cybersecurity compliance issues).

In *Discovery Technologies LLC*, the protester challenged the awardee's ability to meet the requirements of the Federal Information Security Modernization Act (FISMA) under a solicitation that listed FISMA as a law with which the contractor must comply. GAO focused on the solicitation's use of the word "contractor," rather than "offeror," and decided this language supported a determination that FISMA compliance was not required at the time of contract award, but was a matter of contract administration to be addressed by the agency after award (when the "offeror" became the "contractor"). Further, the solicitation did not specifically require that offerors demonstrate compliance with FISMA in their offers.

Similarly, in *Booz Allen Hamilton*, GAO denied a protest in which the protester challenged an award based on its view that the awardee lacked adequate cybersecurity experience. GAO found that the agency properly evaluated the awardee's experience in this area and reasonably assessed a weakness for the awardee's cybersecurity experience, but did not document a "significant weakness" or disqualify the awardee.

More recently, GAO denied a protest and upheld an agency's award decision in a case in which the protester asserted that the agency improperly credited the awardee with a "strength" for its proposed cybersecurity approach. GAO found that the awardee properly was given a strength for proposing to incorporate the voluntary NIST

cybersecurity framework (discussed in Part 3 of this series) in addition to the minimum cybersecurity baseline capabilities required by the solicitation. *IPKeys Techs., LLC*, Comp. Gen. Dec. B-414890 et al., 2017 CPD ¶ 311. Thus, as noted above, contractors that can demonstrate full implementation of NIST requirements as well as other voluntary measures to achieve cyber-fitness stand to benefit in agency evaluation and award decisions.

Other Potential Consequences—In addition to being unfavorably evaluated and potentially not selected for award due to insufficient implementation of cybersecurity capabilities, contractors performing under contracts with cybersecurity requirements may face consequences if issues occur during performance. Depending on specific contract provisions, an agency could determine that a contractor is in breach of a contract and terminate for default based on failure to comply with required provisions, including DFARS 252.204-7012.

Additionally, contractors that do not implement required security controls or properly safeguard sensitive data may be subject to suspension or debarment. Pursuant to FAR 9.406-2, a contractor may be debarred for "[v]iolation of the terms of a Government contract or subcontract so serious as to justify debarment, such as (A) Willful failure to perform in accordance with the terms of one or more contracts; or (B) A history of failure to perform, or of unsatisfactory performance of, one or more contracts." FAR 9.406-2(b)(1). Although this penalty is severe, it may be warranted if the contractor fails to safeguard highly sensitive information or knowingly misrepresents compliance with cybersecurity requirements.

Poor contractor security practices may be noted in a contractor performance assessment report (CPAR), which becomes part of the contractor's "permanent record" and may adversely affect its ability to get future work. In addition, a record of unsatisfactory cybersecurity practices could, in an extreme circumstance, lead to a finding that the contractor is not responsible and, thus, not fit to perform a certain contract.

Finally, it remains to be seen how cybersecurity requirements will be treated under the False Claims Act, which can impose hefty penalties for contractors that submit claims for payment after erroneously certifying compliance with certain requirements. 31 USCA §§ 3729–3733. DOD has made clear that a contractor's signature on a contract represents an agreement to comply with all cybersecurity provisions in that contract, including, where applicable, DFARS 252.204-7012. See DOD FAQs No. 25. Further, a contractor's SSP or other cybersecurity commitments may be part of the technical proposal that is incorporated into the contract, rendering it binding on the contractor and presenting potential liability under the FCA if willfully, recklessly or indifferently ignored.

As we have stressed throughout this series, a contractor's best defense against potential liability is a comprehensive, organized and well-documented approach to cybersecurity. This includes a keen understanding of each contract and the requirements imposed by applicable cybersecurity provisions, as well as clear procedures to be followed in the event of a cyber incident.

Conclusion—At this point, contractors should be close to full implementation of the myriad security controls set forth in NIST SP 800-171, in accordance with DFARS 252.204-7012. DOD understands that implementation of the requirements and the potential consequences for noncompliance seem daunting, and has provided resources to assist contractors. These resources include (1) DOD's "Procurement Toolbox," available at *dodprocurementtoolbox.com,* with various materials, including FAQs relating to the DFARS clauses (with updated FAQs "coming soon"); and (2) a free cybersecurity evaluation tool (CSET) developed by DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), available at *ics-cert.us-cert.gov/Downloading-and-Installing-CSET*. In addition, NIST recently published (1) NIST Handbook 162, a "Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements" for "U.S. manufacturer[s] who supply products within supply chains for the DOD" (available at *nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf*) and (2) its draft version of NIST SP 800-171A, which is meant to "help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in Special Publication 800-171" (available at *csrc.nist.gov/publications/detail/sp/800-171a/draft*).

Although compliance with the NIST publication, demonstrated through an SSP and plans of action, should help to prevent breaches or adverse agency action, remember—*compliance does not equal security*. The DFARS clause recognizes this in its mandate that contractors implement "other information systems security measures," above and beyond NIST SP 800-171, that are reasonably necessary to provide adequate security. But this sentiment is not limited to protecting CDI under the DFARS provisions—contractors should know their data and understand applicable requirements, including data-specific and agency-specific regulations that may not be spelled out in a contract, as well as additional protections that can provide added security.

Do not think that just because you currently do not contract with DOD, you are in the clear. As discussed in Part 2 of this series, the National Archives and Records Administration's rule relating to CUI requires executive agencies to include NIST SP 800-171 compliance in contracts involving CUI in a nonfederal system. This rule promised a FAR case that will make compliance with NIST SP 800-171 a requirement in all civilian agency contracts in which CUI is housed in nonfederal systems. So it is likely all contractors will very soon be subject to the NIST SP 800-171 security controls for contracts that involve CUI.

Achieving cyber-fitness does not admit of a "one-size-fits-all" solution. It is an ongoing process that requires planned, periodic assessments, and updates to stay abreast of evolving cyber threats. We hope this series has provided helpful, practical guidance to assist contractors in achieving cyber-fitness, and has raised awareness regarding the numerous regulations and obligations contractors need to address in implementing effective measures to safeguard sensitive data and to prevent, to the greatest extent possible, the devastating consequences that can result from a cyber attack.

✦

This Feature Comment was written for The Government Contractor by* John Chierichella *and* Townsend Bourne. *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 is an associate in Sheppard Mullin's Washington, D.C. office and a member of the Government Contracts, Investigations, and International Trade practice group. They can be reached at jchierichella@sheppardmullin.com and tbourne@sheppardmullin.com, respectively.

Developments

¶ 364

GAO Urges OMB To Improve IT Reporting And CIO Oversight

The Office of Management and Budget has reported on the highest-priority information technology programs, but the Government Accountability Office November 21 recommended that OMB issue quarterly reports, as required, and ensure that the federal chief information officer is involved in overseeing high-priority IT programs. "Based on the positive impact of direct Federal CIO involvement in leading investment reviews in the past, such involvement could significantly improve program outcomes."

Since 2015, OMB has been required to identify for Congress the 10 highest-priority IT programs in development and submit quarterly status reports, and in 2016, Congress directed OMB's U.S. Digital Service (USDS) to report quarterly on its projects. USDS was established within OMB in 2014.

E-Gov—OMB's Office of E-Government and Information Technology (E-Gov) reported on the 10 highest-priority IT programs in June 2015 and June 2016. E-Gov culled its list from a longer list of "high-impact programs" across agencies, which already require additional oversight. GAO reported that e-Gov's "approach was not guided by any documented procedures or scoring techniques to distinguish the programs." Rather, e-Gov selected the highest-priority programs based on program data, IT dashboard updates, risk exposure, public impact, criticality to agency mission, cost and other factors.

GAO noted that the federal CIO is not involved in oversight of high-impact programs, although "CIO-led TechStat reviews of IT investments performed in 2010 resulted in $3 billion in savings and cost avoidance." See 53 GC ¶ 415.

GAO found that E-Gov's 2015 and 2016 reports provided the status and major milestones of the 10 highest-priority programs, but reports were not issued quarterly, as directed. E-Gov personnel said that competing reporting requirements and limited resources hindered them from issuing quarterly updates.

OMB stopped issuing the reports after June 2016 because it understood the 2016 legislative direction to USDS to report on its projects as superseding the prior reporting requirement. GAO maintained that "continued identification and reporting on the top ten high priority programs, and not just USDS projects, would further enhance congressional oversight by providing congressional stakeholders with information on high priority programs that is not readily available."

USDS—USDS issued reports in December 2016 and July 2017. The reports detailed the status of USDS projects and Government-wide initiatives. USDS staff said they did not issue the reports on a quarterly basis because of the time and effort required.

GAO noted examples of USDS projects, including the Department of Veterans Affairs' *Vets.gov* project to develop a digital healthcare application and the Department of Defense's Defense Travel System to facilitate DOD employee travel. USDS initiatives seek to modernize procurement processes, develop federal shared services and hire top technical talent. USDS' second report included new projects, including a transformation of federal IT procurement through digital IT acquisition training and a project to modernize the Small Business Administration's certification process for small business contractors.

Recommendations—GAO recommended that OMB (1) ensure the federal CIO is directly involved in overseeing high-priority programs; (2) continue reporting on the top 10 high-priority IT programs, including issuing quarterly reports; and (3) continue reporting on the status of USDS projects, including issuing quarterly reports. OMB did not specifically agree or disagree with GAO's recommendations, but expressed "concerns with GAO's alternative interpretations of law" regarding continuing E-Gov and USDS IT reporting requirements.

Information Technology: OMB Needs to Report On and Improve Its Oversight of the Highest Priority Programs (GAO-18-51) is available at *www.gao.gov/assets/690/688504.pdf*.

¶ 365

DHS IG Finds Poor Controls Over Coast Guard IT Acquisitions

The U.S. Coast Guard lacks sufficient controls to determine the appropriate level of oversight required by its non-major information technology acquisitions, the Department of Homeland Security inspector general has reported. "These control weaknesses affect the Coast Guard's ability to effectively oversee non-major IT programs." According to the IG, the Coast Guard spent about $1.8 billion on IT procurements in fiscal years 2014–2016, but does not know if its nearly 400 information systems are receiving proper acquisition oversight because it has been unable to identify all non-major IT acquisition programs among the 400 information systems.

"Major acquisition programs receive Department-level oversight and have historically received a greater level of review," the IG explained. "In contrast, non-major acquisition oversight is primarily delegated to the component and generally receives less scrutiny than major acquisition programs; yet, these programs also encompass investments that have significant systems integration, high risk, or require high performance parameters." The Coast Guard's "controls over IT investments lack synergy and create weaknesses that affect its ability to adequately identify, designate, and oversee non-major IT acquisition programs," the IG warned.

The report attributed the shortcomings specifically to having separate acquisition and IT review processes, limited collaboration between various directorates, outdated and insufficient guidance and IT manuals, insufficient controls for determining the appropriate level of oversight for IT acquisitions, and lack of reliable information on whether information systems may need increased oversight. The Coast Guard has an acquisition

directorate responsible for delivering needed capabilities and a command, control, communications, computers and IT (C4IT) directorate, which designs, deploys and maintains its IT systems and certifies acquisition project conformance with various requirements.

The lack of coordination between the acquisition and IT review processes "risks redundancy in documentation and does not provide a comprehensive layered process for IT acquisitions," the IG added. In FY 2015, the Coast Guard scrapped a plan to modernize its electronic health records system after spending around $68 million because of delays and cost overruns, the IG pointed out. "Programs that do not receive adequate oversight are at risk of wasting money, missing milestones, and not achieving performance requirements."

And because the acquisition and IT review processes operate independently, "if a sponsoring office does not identify a potential non-major acquisition program, there are no processes within [other] directorates to ensure that the investment is reviewed to determine appropriate acquisition oversight," the IG said. "Furthermore, the Coast Guard does not require the sponsors to provide documentation of the assessment performed to determine whether an IT Investment is a potential non-major acquisition."

During the IG review, the Coast Guard established a Non-Major Acquisition Oversight Council to screen acquisition program candidates and provide recommendations for designating IT investments as non-major acquisition programs. Additionally, the IG determined that identifying non-major acquisition programs was "a concern across DHS components." As a result, in March the department began requiring components to "develop a repeatable methodology to identify non-major acquisition programs." The changes "are positive initial steps the Coast Guard needs to take to correct its control weaknesses and ensure it properly identifies IT investments," the IG noted. Implementing these changes also "will improve DHS's visibility over all non-major acquisition programs" and address a recommendation from the Government Accountability Office. "However, the Coast Guard must take additional steps to change the Coast Guard's culture and improve collaboration among directorates for lasting success."

The Coast Guard "must strengthen its controls for identifying and designating non-major IT acquisition programs," the IG concluded. "This includes correcting weaknesses in its guidance, improving coordination between directorates, and implementing preventive controls."

The IG recommended that the Coast Guard (a) analyze acquisition and IT review processes to find redundancies, gaps and potential improvements; (b) evaluate all IT investments and implement a verifiable process to identify non-major acquisitions; (c) ensure that the C4IT directorate develops an up-to-date system for tracking and managing IT investments; and (d) review acquisition and IT guidance to ensure there is a clear process to designate non-major IT acquisitions.

In April, GAO reported that DHS agencies lack the information needed to effectively oversee non-major acquisitions because eight of 11 components could not identify all such acquisitions. See 59 GC ¶ 117. And in May, GAO flagged issues with the DHS chief information officer's oversight of IT contracts. See 59 GC ¶ 166.

Coast Guard IT Investments Risk Failure Without Required Oversight is available at *www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-15-Nov17.pdf*.

¶ 366

GAO Finds Limited Effect Of Kissell Amendment On DHS Textile Purchases

The Department of Homeland Security updated its policies to incorporate legally required restrictions on its procurement of certain textiles, according to a recent Government Accountability Office report. The "Kissell Amendment" was passed as part of the 2009 American Recovery and Reinvestment Act and intended to increase opportunities for American textile and apparel manufacturers. The amendment restricts DHS from using its funds to procure certain fibers, textiles and clothing that are not grown, reprocessed, reused or produced in the U.S.

The Kissell Amendment applies to contracts entered into by DHS as of August 2009. It requires DHS to purchase uniforms made in the U.S. Congress intended the amendment to extend some of the provisions found in the Berry Amendment

to DHS. The Berry Amendment restricts the Department of Defense's procurement of textiles to those produced within the U.S. Under the Kissell Amendment, subject to exceptions, funds appropriated to DHS "may not be used to procure certain textile items directly related to the national security interests of the United States if the item is not grown, reprocessed, reused, or produced in the United States."

Exceptions to the Kissell Amendment include: (1) procurements under the simplified acquisition threshold, currently set at $150,000; (2) instances in which satisfactory quality and sufficient quantity cannot be procured when needed at U.S. market prices; (3) procurements made by vessels in foreign waters or emergency procurements outside the U.S.; and (4) the de minimis exception, in which DHS may accept delivery of a covered item if it contains non-compliant fibers as long as the total value of those fibers does not exceed 10 percent of the total purchase price of the item.

Along with these exceptions, the Kissell Amendment is also to be applied "in a manner consistent with U.S. obligations under international agreements." This means that purchases of Kissell-covered items, including uniforms and body armor, by DHS must be consistent with U.S. obligations under relevant trade agreements. These agreements include the World Trade Organization Government Procurement Agreement and 14 bilateral or regional free trade agreements with 20 countries. These agreements require each party's goods and services to be given treatment comparable to what is given to domestic goods and services in certain Government procurements.

In August 2009, DHS updated the Homeland Security Acquisition Regulation to incorporate the Kissell Amendment restriction on the procurement of textiles from foreign sources. DHS inserted the language into 11 uniform and body armor contracts GAO reviewed. DHS officials told GAO that contracts for the procurement of uniforms and body armor are their only contracts for textile-related products that are directly related to national security interests.

DHS employs multiple procedures to ensure that the restriction on the procurement of foreign textiles from the Kissell Amendment is properly applied, including (a) a standardized procurement contract review process, (b) a requirement for all DHS components to use established department-wide contracts, (c) verification procedures to ensure the stated country of origin is correct, and (d) trainings on foreign procurement restrictions.

GAO concluded that, in practice, the Kissell Amendment affects DHS textile purchases in a limited manner. For most DHS components, the Amendment affects foreign textile procurements directly related to U.S. national security interests that fall between $150,000 and $191,000. GAO reported that from October 2009 to June 2017, only 14 DHS-awarded textile contracts, excluding the Transportation Security Administration, fell within this range. TSA textile procurements, unlike most DHS procurements, are excluded from the coverage of most U.S. international agreements. Therefore, the Kissell Amendment restricts TSA's procurement of certain foreign textiles above $150,000 from all but three foreign countries.

As of June 2017, 58 percent of the value of uniform items ($164.6 million) ordered by DHS came from foreign sources. DHS officials told GAO that the current body armor contracts source all textile items from the U.S.

Government Procurement: Effect of Restriction on DHS's Purchasing of Foreign Textiles Is Limited (GAO-18-116) is available at *www.gao.gov/assets/690/688512.pdf*.

¶ 367

Contract Management Still A Key Challenge, Agency IGs Report

Contract oversight and management remain key challenges for fiscal year 2018 at the departments of Defense, State and Justice, according to annual reports recently issued by those agencies' inspectors general.

DOD—"Acquisition and contract management have remained high-risk areas for … many years, and delivering weapons and technology systems on time and within budget continues to pose major management challenges" to DOD, according to the IG. Despite attempted reforms, many programs "fall short of cost, schedule, and performance expectations," and the department "regularly pays more than anticipated, buys less than expected,

and in some cases, delivers less capability than its contracts require."

"In addition, the Defense Acquisition System often focuses on near-term costs, schedule, and performance trade-offs to the detriment of long-term costs," the IG pointed out. "Yet, more than 70 percent of the life-cycle costs of a weapon system are incurred in the operation and sustainment of the weapon system." DOD's challenges managing contracts for goods and services include overseeing contracting officer's representatives, making payments, and assessing and reporting on contracting performance. And "decision makers sometimes lack information on past and anticipated future contracted services and sometimes focus more on processing the contract action than evaluating the underlying need for the service," the IG warned. "Compounding the acquisition and contracting challenges is the external threat targeting U.S. technologies—specifically, foreign attempts to obtain sensitive or classified information and technologies."

Other key concerns for DOD include addressing challenges in overseas contingency operations, increasing the department's cyber presence and cybersecurity, identifying and implementing efficiencies, and managing strategic challenges from North Korea and other nations.

State—For State, oversight of contracts, grants and foreign assistance is one of six major challenges the department faced in FY 2017, the IG reported. State "must ensure that contractors and grantees are appropriately selected, work is properly conducted and monitored, objectives of the grant or contract are achieved, and costs are effectively contained." Specific concerns include ensuring proper invoice review and approval processes, and monitoring and documenting contractor performance. "Managing contracts and grants can [also] be particularly challenging" during overseas contingency operations, the IG added.

Workforce management also affects contract management, and the IG has found that "inexperienced staff, insufficient training, and staffing gaps and frequent turnover contribute to … other management and performance challenges." For example, construction deficiencies at the U.S. embassy in Kabul "were in large part a result of poor quality assurance and oversight of the construction process." In another case, the IG determined that "personnel responsible for overseeing contracts related to fuel acquisition in Iraq lacked contract-administration experience and technical expertise," which "contributed to oversight deficiencies leading to millions of dollars in questioned costs stemming from fuel purchases that did not conform to quality standards specified in the contract."

"Inadequate oversight and mismanagement pose substantial financial risk to the Department," the IG concluded. "Moreover, oversight weaknesses and mismanagement also increase the possibility that the purpose of these instruments will not be met." The IG also found "grants management practices that did not comply with Department requirements," such as "missing performance or financial reports; insufficient site visits; improper closeout procedures; and a lack of pre-award evaluation criteria, risk assessments, and monitoring plans." In FY 2016, State obligated over $15 billion for contracted services and over $18 billion for grants and fixed charges, the IG noted.

DOJ—Challenges facing DOJ include "the administration and oversight of its contracts and grants," which "create a heightened risk of fraud, waste and mismanagement," according to the IG. Compounding the oversight challenge is that 27 percent, or $1.95 billion, of DOJ contracts in FY 2017 were high-risk time-and-material and labor-hour contracts, the IG said. In FY 2017, DOJ awarded nearly $7.4 billion in contracts and had over $3.5 billion available for grants and cooperative agreements.

"As [DOJ] relies more on the use of contracts and the awarding of grants to fulfill its mission, it becomes increasingly important for it to develop the expertise necessary to administer contracts and its grant programs efficiently, effectively, and in accordance with both federal regulations and Department policy," the IG explained. However, "human capital constraints, decentralized contracting functions, and a lack of adequate monitoring frameworks, such as training and formal policies, often impede the Department's oversight of contractors."

DOJ must also address cybersecurity, which the department designated as its top challenge in its strategic report covering FYs 2014–2018, and its aging information technology infrastructure, the IG noted. DOJ is seeking nearly $31 million

for FY 2018 to address IT modernization, cybersecurity, information sharing technology and related staffing.

DOJ must also manage the federal prison system in the face of declining resources, the IG said. Staffing challenges, particularly at private facilities contracted by the Bureau of Prisons and the U.S. Marshals Service, "aging facilities, and tightening budgets present constant challenges for the BOP in carrying out its mission to confine offenders in safe, humane, and cost-efficient environments," the IG noted. In February, DOJ said it would "continue to use private prisons to house federal inmates." See 59 GC ¶ 54(c). "The BOP and [DOJ] face the challenge of effectively overseeing these private prisons, and ensuring that they are providing the level of staffing, security, and programs that the contracts require."

Contract management was also identified as a key challenge in last year's reports by the State and DOJ IGs. See 58 GC ¶ 415.

The DOD, State and DOJ IG reports are available, respectively, at *media.defense.gov/2017/Nov/20/2001846364/-1/-1/1/FY%202018%20MANAGEMENT%20CHALLENGES_11172017.PDF*; *oig.state.gov/system/files/fy_2017_department_management_challenges_-_508_version_for_publication.pdf*; and *oig.justice.gov/challenges/2017.pdf*.

¶ 368

Developments In Brief ...

(a) Pilot Program to Allow Longer-term Multiyear Procurements—The Department of Defense will carry out a pilot program allowing up to 10-year multiyear procurement (MYP) contracts for certain services under § 854 of the National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, and the Congressional Research Service issued a primer on MYP. Congress has passed the bill, and the president is expected to sign it. See 59 GC ¶ 357. CRS explained that MYP authorizes DOD to use a single contract for multiple years' worth of procurement, and Congress must approve each use. For a typical contract with options, the military service "is under no obligation to exercise any of the options, and a service can choose to not exercise an option without having to make a penalty payment to the contractor," CRS noted. MYP contracts are typically limited to five years. See 10 USCA §§ 2306b(k), 2306c(a). The pilot authorizes up to five longer-term MYP contracts for services specified in 10 USCA § 2306b(b), including (1) facility operation and maintenance; (2) maintenance or modification of aircraft, ships, vehicles, and other complex military equipment; (3) specialized training; (4) base services; and (5) environmental remediation. In addition to the pilot program, § 126 provides authority for MYP contracts for up to seven years for V-22 Osprey tiltrotor aircraft; §§ 123 and 124 provide MYP authority, respectively, for Arleigh Burke-class destroyers and Virginia-class submarines; and § 141 authorizes economic order quantity (EOQ) contracts for the F-35 Joint Strike Fighter. EOQ authority is statutorily included in MYP authority, and CRS described it as "the authority to bring forward selected key components of the items to be procured under the contract and purchase the components in batch form during the first year or two of the contract." CRS periodically updates its MYP primer. See 55 GC ¶ 356; 56 GC ¶ 181. *Multiyear Procurement (MYP) and Block Buy Contracting in Defense Acquisition: Background and Issues for Congress* (R41909) is available at *fas.org/sgp/crs/natsec/R41909.pdf*.

(b) Amtrak Project Faces Oversight and Schedule Risks—The National Railroad Passenger Corp. (Amtrak) should improve program oversight and contractor planning in its program to replace trains in the U.S. northeast corridor and make related infrastructure improvements, the Amtrak inspector general has recommended. In 2016, Amtrak received a loan through the Federal Railroad Administration for the Acela Express 2021 program. Amtrak will purchase 28 high-speed trains for $1.6 billion, conduct 10 infrastructure projects, and pay $850 million to operate and maintain the trains. In September 2016, Amtrak awarded

a multibillion contract to Alstom S.A. for the trains. See 58 GC ¶ 317(d). The trains are scheduled to begin service in 2021, and the infrastructure projects are scheduled for 2018–2021. In July 2017, Amtrak designated its enterprise program management office (EPMO) as the Acela program lead but has not defined EPMO's duties and authorities, the IG found. Amtrak has not staffed a team to oversee the 10 infrastructure projects or implemented an integrated master schedule or a list of risks and mitigation plans for the infrastructure projects. Amtrak has not determined the number and types of safety and track personnel it needs for the infrastructure projects. Such personnel are in high demand across Amtrak, and Amtrak intends to supplement them with contractors. Further, Alstom has reported that the trains are 81–89 days behind schedule for redesign work to meet crash-protection standards. Amtrak officials believe that Alstom can recover from the delay, but Alstom said it has already been mitigated as much as possible. The IG recommended that Amtrak (a) define EPMO's authorities, (b) develop an Acela integrated master schedule, (c) determine the number of Amtrak and contractor personnel needed, (d) review its plans to use contractors, and (e) staff a team to manage the infrastructure projects. Amtrak is a federally chartered corporation, established by the Rail Passenger Service Act of 1970. *Train Operations: The Acela Express 2021 Program Faces Oversight Weaknesses and Schedule Risks* (OIG-A-2018-002) is available at *www.amtrakoig.gov/sites/default/files/reports/OIG-A-2018-002.pdf*.

(c) IG Passes DCAA Quality Control System Despite Deficiencies—The Department of Defense inspector general recently reviewed the Defense Contract Audit Agency quality control system and found that it "has been suitably designed and complied with to provide DCAA with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects." A quality control system is designed to ensure that the organization and its personnel comply with professional standards and legal requirements. Although the system passed, the IG did find evidence of reporting, documentation, supervision and professional judgment deficiencies within the system. DCAA disagreed with the "pass with deficiencies" opinion and in its response to the report said that the reporting, supervision and professional judgment deficiencies found "did not rise to the level of a system-reportable deficiency as defined in the Council of the Inspectors General on Integrity and Efficiency (CIGIE) guidance." DCAA also believes that the IG "overstated the conclusions by citing the same funding under several deficiencies." The IG responded that its reported deficiencies qualify as system-reportable deficiencies as defined in the CIGIE guidance which defines a deficiency as

> one or more findings that the review team has concluded, due to the nature, causes, pattern, or pervasiveness, including the relative importance of the finding to the OIG audit organization's system of quality control taken as a whole, could create a situation in which the organization would not have reasonable assurance of performing and/or reporting in conformity with applicable professional standards in one or more important respects.

External Peer Review on the Defense Contract Audit Agency System Review Report (DODIG-2018-028) is available at *media.defense.gov/2017/Nov/22/2001847672/-1/-1/1/DODIG-2018-028.PDF*.

(d) IG: VA Did Not Reimburse Treasury for CDA Claims, as Required—The Department of Veterans Affairs did not reimburse the Treasury Judgment Fund, as required by statute, after the Department of the Treasury used the fund to pay 23 Contract Disputes Act claims "related to 10 major medical facility construction projects totaling $247,748,686, with an average payment delinquency of 221 days," the VA inspector general has reported. As of January 31, over $226 million, or 91 percent, remained unpaid. According to the IG, the VA has been delinquent because the

department considered reimbursing the funds a lower priority than requirements that support veteran access and safety, and the VA has not been seeking sufficient funding for the reimbursement of CDA claims. For example, although the VA had an overdue balance of over $226 million, its fiscal year 2017 congressional request for reimbursing the Judgment Fund for the payment of claims was only $9 million, the IG pointed out. By not making timely reimbursement payments, the VA has "continued to maintain significant liabilities not covered by budgetary resources," and the department "will require significant future funding to satisfy the outstanding claims." The IG recommended that the VA either establish procedures to make reimbursement payments within 45 days of receiving demands for reimbursement or make appropriate payment plans for CDA claims. *Review of VA's Reimbursements to the Treasury Judgment Fund* is available at *www.va.gov/oig/pubs/VAOIG-17-00833-05.pdf*.

(e) State COs Can Improve Afghan Antiterrorism Oversight—The Department of State should ensure that contracting officers and CO's representatives properly oversee its Antiterrorism Assistance (ATA) program in Afghanistan, the State inspector general has recommended. State's ATA programs are intended to enhance allies' antiterrorism skills, strengthen bilateral ties between the U.S. and other countries, and increase respect for human rights. The Afghanistan ATA program is implemented by State's bureaus of Diplomatic Security and Counterterrorism. State officials said that "competing priorities" have prevented them from implementing a robust ATA program monitoring and evaluation system, as the IG has previously recommended. State has not been collecting formal Afghanistan ATA reports, required by the Global ATA contract, because the CO "elected to receive weekly phone conferences rather than formal, written reports." And in-country oversight was limited because "[t]he in-country deputy program manager, who was a third-party contractor, was overseeing training in the field, but could not be designated as a COR or [Government technical monitor] because contractors (other than personal services contractors) are not eligible to fill those roles." The IG recommended that State (1) require COs and CORs overseeing ATA programs to document progress from phone conferences in lieu of formal reports, (2) implement a monitoring and evaluation system, (3) verify that CORs have documentation to support invoices, (4) verify that COs issue written contract modifications when necessary, and (5) verify compliance with reporting requirements. The IG also found that State made some progress in its Afghan ATA program, including periodically validating a database for tracking equipment and implementing a process to ensure equipment compatibility. *Management Assistance Report: Although Progress Has Been Made, Challenges Remain in Monitoring and Overseeing Antiterrorism Assistance Program Activities in Afghanistan* (AUD-MERO-18-16) is available at *oig.state.gov/system/files/aud-mero-18-16.pdf*.

(f) GAO Surveys FY 2017 ADA Violations—The Government Accountability Office has issued its fiscal year 2017 report on violations of the Antideficiency Act. The ADA prohibits federal employees from authorizing expenditures or obligations in excess of appropriations or before appropriations have been made. See 31 USCA §§ 1341–1342, 1517. Agencies reported 16 ADA violations to GAO in FY 2017, and GAO reported the violation amounts, dates, agency and remedial actions, if any. Violations with the largest dollar values were for (a) $437.9 million by the Commodity Futures Trading Commission, which incurred obligations on multiple-year real estate leases and accepted voluntary lease services in FYs 1995–2015, when it failed to notify two landlords that appropriations were available for its leases; (b) $93.5 million by the Army in FY 2012, for obligating funds to develop software from an improper account and for reprogramming funding not legally available for obligation; and (c) $77.5 million by the Air Force for multiple surcharges on technology

transactions without legal authority in FYs 2007–2010, resulting in augmentation of the Air Force's operations and maintenance account. Upon discovering an ADA violation, an agency is to report it immediately to the Office of Management and Budget, Congress and the U.S. Comptroller General. See 31 USCA §§ 1351, 1517(b). In 2009, GAO interpreted the ADA as applying to all statutory restrictions on the amount of spending or on purposes for which appropriations can be used. See *Antideficiency Act—Applicability to Statutory Prohibitions on the Use of Appropriations*, Comp. Gen. Dec. B-317450, 2009 CPD ¶ 72; 51 GC ¶ 135. GAO declined to follow the conflicting 2007 opinion of the Department of Justice office of legal counsel that the ADA applies to restrictions only in appropriations acts, not in other statutes. GAO's FY 2017 ADA report is available at *www.gao.gov/assets/690/688415.pdf*.

Regulations

¶ 369

ABA Section Recommends Acquisition Regulation Improvements

The American Bar Association's Section of Public Contract Law has submitted comments to the Department of Defense's Section 809 Panel on streamlining and improving acquisition regulations. The ABA section made recommendations to improve Federal Acquisition Regulation and Defense FAR Supplement rules on cybersecurity, novation agreements, contractor team arrangements, and weighted guidelines for negotiating profit objectives.

Cybersecurity—The ABA section criticized DOD's implementation of DFARS interim and final rules on network penetration reporting. See 58 GC ¶ 387. DOD "essentially asked contractors to comply with an entirely new information-security framework, with complex and demanding requirements, immediately," the ABA section admonished. It recommended that DOD ensure that new cyber- and information security rules allow sufficient time for contractors to incorporate them in internal systems.

The ABA section recommended ensuring that cybersecurity reporting requirements are feasible. It noted that "many states provide substantially longer timeframes or more situation-dependent timeframes such as 'without undue delay,' instead of a flat 72-hour window" in the abovementioned DFARS rule.

The section also recommended that DOD consider the impact on small and medium-sized contractors, and emphasized the "continued need for ongoing education within the Government on the intended operation" of the DFARS rule. "[I]t would help for DoD to have developed underlying and related guidance such as how to identify and mark controlled unclassified information before requiring contractors to comply with and flow down requirements contingent on these definitions."

The ABA section submitted similar comments to a DOD task force on eliminating unnecessary DFARS clauses. See 59 GC ¶ 294. It previously submitted comments critical of the DFARS interim rule. See 57 GC ¶ 382; 57 GC ¶ 392.

Novation Agreements—The FAR 42.1204 requirements on novation agreements are "outdated, inconsistent with commercial practices, and often incongruent with market realities," the ABA section said.

In private mergers and acquisitions (M&A), the parties can quickly "assign" contracts, but Government novations can take years to finalize. The discrepancy can necessitate temporary pass-through subcontracts, pending finalization of the novation agreement. "These structures may be complex and confusing for all sides and do not serve anyone's best interests," the section explained.

DOD should allow contractors to begin the novation process before the M&A transaction is closed. "Because novation can be requested only after a transaction has closed, parties must complete their transaction before they can formally ask the Government for permission to complete a transaction that was just completed." Further, the unlimited timeline for processing novations creates undue uncertainty. The ABA section recommended a 90-day requirement for federal officials to approve or disapprove novation applications—

similar to deadlines for Committee on Foreign Investment in the U.S. review deadlines.

The ABA section urged DOD to simplify the required contents of the novation package. "Eliminating even some of the unnecessary documentation will shorten that process without increasing government risk," and some required documents "are superfluous and appear often times to not be reviewed by government personnel." Similarly, DOD should eliminate the "cumbersome, outdated, and often waived" requirement for pre- and post-M&A audited financials. DOD should replace it with "a requirement to provide financial evidence of the buyer's ability to perform in its capability statement."

Team Arrangements—"There is an unjustified concern that exclusive team arrangements are anti-competitive," the ABA section said of contractor team arrangements under FAR subpt. 9.6. It recommended that DOD "let market forces determine whether and to what extent exclusivity in a particular arrangement makes commercial as well as competitive sense."

"[C]ontracting agencies should not prohibit or place heavy burdens on team arrangements," the section said, noting that the Federal Trade Commission and Department of Justice have recognized the benefits of teaming agreements and issued guidelines. It is not in DOD's or industry's interests "to discourage the formation of team arrangements that allow firms to combine their complementary technological know-how and manufacturing capabilities to best meet the Government's needs."

Weighted Guidelines—The ABA section recommended that DOD revise the weighted guidelines method of negotiating profit objectives under DFARS 215.404-4 and -71. The current regulations often lead to a price-negotiation impasse by preventing contracting officers from agreeing to price terms early on. Instead, COs should be encouraged to agree on terms as early as possible so that technical evaluators can assess the contractor's proposed weighted guidelines terms.

DOD should also revise the rules to provide for contractors to use the same weighted guidelines system as COs, "so that both parties are comparing data sets based on the same algorithms." If the weighted guidelines do not yield an agreement, COs should be authorized to request profit history for similar contracts to assess what the contractor has agreed to as reasonable profit. "Contractors should not be required to provide the profit information if requested, but should be allowed to determine for themselves whether it is in their best interest to do so," the ABA section said.

The ABA section submitted similar recommendations on weighted guidelines to the DOD DFARS task force. See 59 GC ¶ 294.

The Section 809 Panel was established by § 809 of the National Defense Authorization Act for Fiscal Year 2016, as amended by § 863 of the FY 2017 Defense Authorization Act. See 58 GC ¶ 357(b). In May, it issued its interim report, and panel members testified before the House Armed Services Committee. See 59 GC ¶ 160.

The ABA section's comments are available at *www.americanbar.org/groups/public_contract_law.html*.

Decisions

¶ 370

CICA Exemption Precluded GAO Protest Jurisdiction

A-Z Cleaning Solutions, Comp. Gen. Dec. B-415228, 2017 CPD ¶ 343

By statute, the U.S. Mint is exempt from "provisions of law governing procurement" and "public contracts" and is therefore not subject to the Competition in Contracting Act (CICA) and the Government Accountability Office's CICA-based protest jurisdiction, the U.S. Comptroller General recently held.

A-Z Cleaning Solutions protested the award of a contract under a Mint solicitation for janitorial and laundry services. CICA gives GAO jurisdiction over bid protests concerning solicitations and contract awards issued "by a Federal agency." 31 USCA § 3551(1). CICA adopts the definition of "federal agency" in 40 USCA § 102, which states that "federal agency" includes any "executive agency," defined as any "executive department or independent establishment in the executive

branch of the government." 40 USCA § 102(4), (5). The Mint, part of the Department of the Treasury, is an executive agency that otherwise would come within GAO's protest jurisdiction under CICA.

In 1996, however, Congress established the U.S. Mint Public Enterprise Fund (USMPEF) to finance Mint programs and operations. The establishing legislation stated that "provisions of law governing procurement or public contracts shall not be applicable to the procurement of goods or services necessary for carrying out Mint programs and operations." 31 USCA § 5136. The same provision defines Mint programs and operations broadly enough to include substantially all Mint activities. That provision also contemplates that receipts from Mint operations and programs are deposited in the USMPEF for use in paying Mint expenses.

Because the establishing legislation provides that federal procurement laws and regulations do not apply to substantially all Mint operations and programs, the Mint is not subject to CICA and therefore not within GAO's protest jurisdiction, the Comp. Gen. said.

The Comp. Gen. rejected the protester's argument that because the Treasury has a similar, but narrower exemption from procurement statutes for the production of listed numismatic items, see 31 USCA § 5112, the exemption in 31 USCA § 5136 should be read to apply only to numismatic items. That argument ignored the differences between activities governed by § 5112 and those covered by § 5136, and ignored § 5136's explicit list of exempt Mint operations and programs.

The Comp. Gen. has similarly concluded that other CICA-exempt entities are not within GAO jurisdiction. See *Falcon Sys., Inc.*, Comp. Gen. Dec. B-222549, 86-1 CPD ¶ 462 (U.S. Postal Service); 28 GC ¶ 191 (Note); *Performance Excavators, Inc.*, Comp. Gen. Dec. B-291771, 2003 CPD ¶ 63 (Presidio Trust, a wholly owned Government corporation).

The Comp. Gen. distinguished agencies that are within GAO protest jurisdiction because they are not exempt from CICA provisions providing GAO protest jurisdiction although they are exempt from the substantive provisions of basic procurement statutes, such as the Armed Services Procurement Act and the Federal Property and Administrative Services Act (FPASA), both of which were amended by CICA. See, e.g., *Gino Morena Enters.*, Comp. Gen. Dec. B-224235, 87-1 CPD ¶ 121 (Air Force procurement of a concession financed with nonappropriated funds); *Starfleet Marine Transp., Inc.*, Comp. Gen. Dec. B-290181, 2002 CPD ¶ 113 (procurement conducted under alternative procedures authorized by statute and not subject to FPASA requirements); 44 GC ¶ 285; *Superior Reporting Servs., Inc.*, Comp. Gen. Dec. B-230585, 88-1 CPD ¶ 576 (Administrative Office of the U.S. Courts); cf. *MFM Lamey Group, LLC*, Comp. Gen. Dec. B-402377, 2010 CPD ¶ 81 (statute authorizing agency to take certain actions notwithstanding any other provision of law that does not expressly exempt an agency from procurement statutes or authorize alternative procurement procedures does not exempt agency from basic procurement statutes or GAO protest jurisdiction).

✦ **Note**—U.S. Court of Federal Claims jurisdiction arises from 28 USCA § 1491 rather than CICA. The different statutory basis for jurisdiction can result in broader COFC protest jurisdiction. For example, as the Comp. Gen. noted in *A-Z*, GAO lacks jurisdiction over Postal Service procurement protests. In *Emory Worldwide Airlines, Inc. v. U.S.*, 264 F.3d 1071 (Fed. Cir. 2001); 43 GC ¶ 351, the Court of Appeals for the Federal Circuit detailed the development of COFC protest jurisdiction and interpreted COFC jurisdiction under § 1491 to include Postal Service protests. The Federal Circuit's decision turned on the definition of "federal agency" applicable to COFC jurisdiction under § 1491. See 28 USCA § 451. See also *Office Depot v. U.S.*, 95 Fed. Cl. 517 (2010) (Federal Deposit Insurance Corp. is an agency within COFC protest jurisdiction).

¶ 371

Aircraft-Capacity Maximum Unduly Restricted Competition, Comp. Gen. Says

Global SuperTanker Servs., LLC, Comp. Gen. Dec. B-414987 et al., 2017 CPD ¶ 345

A solicitation's restriction on maximum aircraft tank capacity unduly restricted competition, and

the agency did not show that the restriction was reasonably necessary to meet its needs, the U.S. Comptroller General has determined. Although "the agency is entitled to great discretion in establishing its needs … the agency has failed to provide reasonable justifications for the challenged specification."

In May 2017, the Forest Service issued a request for proposals for multiple "call when needed" basic ordering agreements (BOAs) for large airtanker (LAT) services for "initial" and "extended" attack phases in fighting wildfires. Consistent with prior solicitations, the RFP required a minimum tank capacity of 3,000 gallons of flame retardant, but in a footnote, the RFP included a new requirement limiting the maximum tank size to 5,000 gallons.

Global SuperTanker Services LLC (GST) owns the Spirit of John Muir, a very large airtanker (VLAT). GST protested the 5,000-gallon restriction to the Forest Service, which denied the protest, stating that VLATs are "not ideal for initial attack purposes" and citing four Forest Service studies. GST then protested to the Government Accountability Office, arguing that the maximum tank-size requirement was unduly restrictive of competition and not reasonably necessary to meet the Forest Service's needs.

A VLAT competitor and the only other tanker-service provider with tankers greater than 5,000 gallons, 10 Tanker Air Carrier LLC, sought to intervene because it intended to bid on a related Forest Service RFP that would include the same maximum-capacity restriction. Because 10 Tanker did not intend to bid on the instant solicitation, the Comp. Gen. denied its request to intervene, but GST included in its filings statements and documents from 10 Tanker.

Restricting Competition—Procuring agencies "may include restrictive requirements only to the extent they are necessary to satisfy legitimate needs," the Comp. Gen. said, citing *Parcel 49C Ltd. P'ship*, Comp. Gen. Dec. B-412552 et al., 2016 CPD ¶ 95. The Comp. Gen. reviews an agency's explanation of restrictions "for reasonableness, that is, whether it can withstand logical scrutiny." See *Pitney Bowes, Inc.*, Comp. Gen. Dec. B-413876.2, 2017 CPD ¶ 56.

Preliminarily, the Comp. Gen. emphasized that "call when needed" BOAs provide "the ultimate flexibility," not requiring an agency to place any orders and incurring no costs for inactive days. Thus, "it costs the Forest Service nothing to permit the inclusion of VLATs in the subject procurement, while simultaneously increasing the agency's available options during fire season."

Initial Attack Operations—The Forest Service argued that VLATs do not meet its needs for both initial and extended attacks. However, the Forest Service's denial of GST's agency-level protest focused solely on VLATs' inability to meet initial attack needs. The Comp. Gen. found this to be a post hoc attempt to justify the 5,000-gallon restriction, and the Forest Service's "conclusion that VLATs are not suited for initial attack operations does not provide a reasonable justification for excluding VLATs from the competition where the solicitation also seeks services for extended attack operations."

Nothing in the record indicated who decided to include the 5,000-gallon restriction or why, or even that it "was ever discussed, considered, or recommended by any agency official in the context of this solicitation." And the Forest Service acknowledged that since it began ordering "call when needed" services in 2009, it had never restricted maximum capacity. Furthermore, the Forest Service had recently awarded three initial attack services contracts to 10 Tanker, which would perform the services with 11,600-gallon VLATs. "Thus, the record shows that, until very recently, the agency considered 10 Tanker's VLATs to be capable of performing initial attack operations."

The Comp. Gen. acknowledged that a procuring agency may deviate from prior practice, but "the agency's basis for its requirements must be reasonable where such requirements allegedly restrict competition." See *WingGate Travel, Inc.*, Comp. Gen. Dec. B-405007.9, 2011 CPD ¶ 260.

Studies Cited—The Forest Service cited studies from 1995, 1996, 2005 and 2012, but the studies did not support its position, the Comp. Gen. found. For example, the 2005 study "merely indicates that the agency prefers larger aircraft over smaller aircraft, not that VLATs are somehow less desirable for initial attack operations," and "the 2012 study could be construed to support the protester's arguments."

GST also pointed to an article by a wildlife expert and a GAO report questioning the complete-

ness and accuracy of the Forest Service studies and the data they rely on. In addition, the Comp. Gen. noted that the Forest Service continued using VLATs for initial attack operations for "years, even decades, after the publication of the studies."

Other Arguments—The Comp. Gen. considered various other reasons the Forest Service advanced for excluding VLATs, but it addressed only "a few representative arguments."

The Forest Service said only three bases had capacity to load VLATs without restricting LAT operations. GST countered with a list of 16 bases its VLATs could operate from—and dozens more for specific types of activity, such as water operations—and detailed its process for determining which airfields have VLAT capacity. The Comp. Gen. concluded that the Forest Service "has not reasonably demonstrated that VLATs can only operate out of a small number of bases."

The Forest Service also argued that VLATs are not suited for initial attack because they require lead planes, whose availability is currently limited. GST pointed out that LATs also require lead planes, and the Forest Service did not present any evidence of a shortfall of lead planes. GST also clarified that lead planes are based not on aircraft type, but on pilot qualifications, and GST could begin certifying its pilots as initial attack lead-pilots if it won the contract at issue. Here, again, the Comp. Gen. found that the Forest Service had not demonstrated a need to exclude VLATs.

The Forest Service said VLATs require additional federal personnel. GST argued that a VLAT would necessitate only one federal employee more than an LAT, but because a VLAT replaces several smaller aircraft, the overall need for federal personnel could be less. The Forest Service did not provide any analysis of employee requirements, so the Comp. Gen. found no basis for its assertions.

The Forest Service maintained that VLATs require extra fuel and retardant. GST noted that one VLAT carries more retardant than five to six LATs, such that "prudent use of VLATs will in the aggregate require less fuel than a comparable amount of LATs." Again, the record did not contain evidence that the Forest Service had assessed or compared alternatives. "Here, too, we find that the agency failed to weigh the pros and cons of using VLATs," the Comp. Gen. said. Finally, the Forest Service cited two instances of VLATs damaging airbases. Reports on the incidents, however, showed that they were fully or mostly the fault of Forest Service employees.

GST also said the Forest Service did not consider the cost advantages of VLATs and failed to consider the economies of scale that would make VLATs significantly less expensive than LATs. And GST argued that for a "call when needed" BOA, excluding VLATs was "simply not logical," as the Forest Service could simply not order VLATs if a given wildfire did not require them. Indeed, the RFP and acquisition plan "demonstrate the agency's preference for 'having all qualified airtankers available' and for maintaining flexibility in determining what assets to order," the Comp. Gen. concluded, sustaining the protest and finding that the 5,000-gallon maximum "does not withstand logical scrutiny."

Recommendations—The Comp. Gen. recommended that the Forest Service make a documented determination of needs, and then revise the RFP to include reasonably necessary specifications. It also recommended that GST be reimbursed protest costs and attorneys' fees.

Reminder ...

Thomson Reuters will be hosting its annual Government Contracts Year In Review Conference Feb. 20–23, 2018, at the Omni Shoreham Hotel in Washington, D.C. Inquiries should be directed to Nick Lipkowski at 1.800.922.4330 x28286 or *Nick.Lipkowski@thomsonreuters.com*.

The Government Contractor Advisory Board

THOMSON REUTERS®

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®

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

FIRST CLASS

DATED MATERIAL PLEASE DELIVER PROMPTLY

December 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
24/31	25	26	27	28	29	30

January 2018

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			

February 2018

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			

Administration of Government Contracts
January 30-31
Arlington, VA
$1275

Advanced ITAR
February 16
Las Vegas, NV
$950

Basic ITAR
February 14-15
Las Vegas, NV
$1275

Basics of Government Contracting
January 22-24
McLean, VA
$1350

Basics of Government Contracting
February 5-7
Las Vegas, NV
$1350

Basics of Multiple Award Schedule Contracting
February 22-23
Sterling, VA
$1275

The Buy American & Domestic Preference Workshop
February 22-23
Sterling, VA
$1275

Cost & Price Analysis in Government Contracts
February 21-22
Las Vegas, NV
$1275

FAR Workshop
February 21-22
Las Vegas, NV
$1275

FAR Workshop
January 25-26
McLean, VA
$1275

Government Contract Accounting
January 30-31
Arlington, VA
$1275

A Practical Guide to the Incurred Cost Submission
February 6-7
Sterling, VA
$1275

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*