Government Contracting
Navigating the Land Mines
By Scott Arnold

Budget Limitations Persist

Budget limitations imposed by the Budget Control Act of 2011, including sequestration—the automatic spending cuts imposed as Congress fails to agree on spending priorities—are not going away any time soon. Companies that wish to sell to the federal government in 2015 and beyond should understand that competition for that business is only likely to get more intense.

With programs losing funding or facing elimination altogether, procuring agencies and their auditing and investigative affiliates have come under increasing pressure in recent years to take hard lines in the administration of government contracts. Contractors often lose money on fixed-price contracts that impose too much contractor risk, or face aggressive government claims facilitated by auditors who, as a practical matter, are incentivized to maximize the recovery of dollars for their constituent procurement agencies that are not getting any more from Congress. These contractors sometimes look back at their decision to bid on government contracts in the first place and recall the adage, “be careful what you wish for.”

Is it worth it? It certainly can be. Even though contracting with the government imposes challenges that, as LRN Risk Forecast Reports have previously noted, are not for the faint of heart, the government has purchasing needs that can be as broad as—and in many cases go well beyond the needs of—nongovernmental commercial customers. Opportunities exist to expand markets beyond what would be possible by selling goods and services only to nongovernmental customers, and also to sell products and services for which government agencies may be the predominant or sole customers.

Compliance with the myriad of regulations applicable to government contractors, often through contract clauses imposed by the government at the prime contract level and flowed down to subcontractors, is, of course, essential. Success also requires cognizance of potential risk areas that have surfaced recently and taking prudent steps to manage them.

Cybersecurity—Government Contractors Must Pay Attention

Recent difficulties experienced by the contractor U.S. Investigative Services (USIS) demonstrate that cybersecurity is becoming a pressing issue. Contractors that store sensitive information in the performance of their government contracts must avoid being a “weak link” for potential cyberattackers. USIS, which had already received bad publicity stemming from its background checks on Edward Snowden and Navy Yard shooter Aaron Alexis, and a fraud suit accusing the company of filing incomplete background check reports while billing the government for them, lost its Office of Personnel Management contracts for background check work after cyberattackers breached its data systems.1

Counterfeit Electronic Parts

The Department of Defense Federal Acquisition Regulation Supplement (DFARS) includes a rule finalized in May 2014 that requires certain defense contractors to undertake significant efforts to ensure

Scott Arnold
ECA Affiliate

Scott Arnold is a leading expert in the area of government contracts law and compliance. Scott is a partner in the Law Firm of Dickstein Shapiro LLP, where he specializes in government contracts counseling, litigation and compliance matters. Prior to his nearly 30 years in private practice, Scott served as a procurement attorney in the U.S. Navy’s Office of General Counsel.
that their supply lines do not contain counterfeit electronic parts and to disclose to the government instances where counterfeit parts are suspected.\(^2\) A counterfeit part is defined in the new rule as one that is “knowingly mismarked, misidentified, or otherwise misrepresented.”\(^3\) This is to be distinguished from nonconforming parts, which are parts that do not meet specifications, but do not necessarily involve intent to mislead someone to believe the part is something that it is not.

The new rule has become controversial due in part to disagreement over to whom counterfeit part disclosures must be made. Since the promulgation of the so-called mandatory disclosure provisions in 2009, government contractors have been required to implement ethics programs that provide for the disclosure to an appropriate agency Inspector General (IG) whenever there exists credible evidence of a violation by the contractor or subcontractor of certain criminal laws involving fraud, conflict of interest, bribery or gratuities, or a violation of the civil False Claims Act.\(^4\) In contrast, there is no language in the new DFARS rule requiring that disclosures regarding counterfeit parts actually be made to the Department of Defense (DOD) IG, as opposed to the contracting officer. Nonetheless, the DOD Deputy IG for Policy and Oversight has suggested that all disclosures related to counterfeit parts should go to the DOD IG’s office—a position that has been questioned by some in the government contracts bar.\(^5\)

Has the Deputy DOD IG overreached in asserting that any instance of a counterfeit (or even plain old nonconforming) part must be reported to the IG? Perhaps, but the stance is typical of the current government contracting environment, which often encourages contractors to err on the side of disclosure—or broader disclosure—in close calls.

**Corporate Transactions and Restructuring**

The 2014 LRN Risk Forecast Report noted that, with declining procurement budgets, investors should proceed with caution in assessing whether to acquire government contractors. This certainly remains the case. Companies already involved in government contracting also must take special care when planning corporate transactions or restructuring. A recent Government Accountability Office (GAO) bid protest decision\(^6\) underscored the care needed when a company plans corporate restructuring that will impact how the government contract on which it is proposing will be performed.

In that case, Wyle Laboratories protested a $1.7 billion NASA contract award to Science Applications International Corporation (SAIC) on several grounds, including NASA’s failure to properly consider the ramifications on contract performance of SAIC’s plans to split into two separate companies. NASA and SAIC argued in response that, notwithstanding SAIC’s announced plans for the split, the contract award to SAIC, which took place a few weeks before implementation of the split, was proper because NASA was not in a position to “speculate” about whether the split would actually go through, and thus was justified in disregarding the impending split when evaluating SAIC’s offer.

GAO disagreed and sustained the protest. In so doing, GAO also rejected arguments that because the split did not actually occur until after the contract was awarded to SAIC, the issue was a matter of post-award contract administration that is outside GAO’s jurisdiction. While GAO’s decision may have surprised some in the government contracts community given that no split had occurred when the award was made, the decision was correct. The problem with the award was fundamental—NASA failed to consider a planned split even though it had been publicly announced, was addressed in portions of SAIC’s proposal, and raised numerous questions about how SAIC would actually fulfill the promises made in its proposal.

The lesson for procuring agencies? In evaluating offers, they cannot ignore the ramifications of a post-award transaction that they know or should know is likely to occur simply on the basis of less than 100 percent certainty it will occur. The lesson for contractors is that they need to be extremely careful when planning corporate transactions that may take place after a competitive solicitation ends, and to fully and consistently address the issues this creates in their proposals.
Audit Trends

Companies holding cost-type government contracts or contracts involving the submission of cost and pricing data under the Truth in Negotiations Act (TINA) have been facing increasingly aggressive government audits in recent years. The Defense Contract Audit Agency (DCAA), in particular, is not only questioning greater amounts of its total dollars examined,7 but has often pushed the envelope in access requests that exceed its statutory authority. This has included (1) seeking access to company internal audit reports regardless of whether there is any showing of an actual nexus between the information contained in such reports and a valid DCAA mission, such as the need to evaluate the contractor’s business systems, and (2) requests to interview contractor employees about “actual or suspected fraud.”8

Companies subjected to such requests may face a dilemma. It is generally best for contractors to cooperate with auditors to avoid perceptions that they are impeding audits. However, agreeing to requests that go beyond a DCAA auditor’s legitimate authority could lead to waivers of privileged information and the commencement of investigations based on misunderstandings by auditors who, while generally competent to assess accounting data, may not necessarily be qualified to assess subjective information provided by employees in interviews about possible fraud.

Steps to Best Ensure Success

Although continuing budget cuts loom large and the federal government can be a challenging customer, there are a number of steps that companies can take to improve their chances of success in the government contracts market.

• **Be prepared to deal with bid protests:** Fierce competition for pieces of a smaller pie will likely continue to lead to protests in significant programs. Companies are glad to have a possible protest avenue when they lose, but are unhappy to have their contract work suspended when they win and a competitor protests. Either way, companies are best prepared to deal with protests, and possibly to avoid them, when they proactively consider potential issues well before offers are due and raise any questions about the procurement process with the agency early. If an RFP provision is ambiguous, do not guess what the government wants. Raise questions and get the issue resolved.

• **Do not sit on valid claims:** Tight budgets increase the likelihood that a procuring agency may try to get more than it is entitled to out of a government contract. Contractors must be prepared to communicate concerns to the contracting officer promptly when this appears to be happening. Failure to make timely notification can prejudice a contractor’s ability to recover.

• **Be prepared to deal with inexperienced procurement personnel:** Another unfortunate trend with declining budgets is the increasing challenge the government faces in maintaining a top-notch procurement workforce. Although the federal government has many excellent contracting officers and procurement personnel generally, many are inexperienced, must learn on the job, and are prone to make mistakes. Be patient and learn how to work with such personnel as effectively as possible—you may need to show them the ropes.

• **Be prepared to cooperate with auditors, but also recognize that they sometime overstep their bounds:** Contractors sometimes need to choose between refusing unjustified auditor requests, which entails the risk of alienating the auditor or even being accused of impeding an audit, or simply complying with the request. Making this decision entails an exercise of judgment that accounts for the particular circumstances. Contractors with strong ethics and compliance programs are in the best position to navigate these issues with limited exposure.

• **Enhance quality programs as necessary to comply with the counterfeit electronic parts rules to the extent applicable:** Government contractors subject to the Cost Accounting Standards that sell supplies containing electronic parts to DOD will
need to ensure that they comply with the strict new DFARS rules designed to eliminate counterfeit parts from supplies sold to DOD. Subcontractors under these programs will also need to comply. Even if the counterfeit electronic parts rules are not applicable, it remains important for all government contractors to have effective quality assurance programs.

• **Take cybersecurity seriously:** This past year we saw not only USIS’s loss of government contracts due to a cybersecurity breach, but also China’s aggressive actions in penetrating the networks of established defense contractors. This underscores the risk for future breaches. The government is becoming more explicit in using contract clauses to penalize contractors whose technical solutions prove inadequate to defend against cybersecurity attacks, and to shift significant risk to contractors. Contractors should, of course, do all that is possible to prevent such breaches from taking place.

  However, it may not be possible to completely eliminate the risk of a cybersecurity breach. Contractors should determine whether they can adequately insure for the risks of cyberattacks, and, if not, consider whether contracts entailing the management of sensitive data are too risky.

• **Government contractors planning corporate restructuring need to consider the possible impact this may have on existing contracts and proposals for new work:** As now clear from GAO’s Wyle bid protest decision, a planned corporate transaction that can impact future contract work needs to be adequately and consistently addressed in the proposal for that future work, regardless of whether the transaction ultimately takes place before or after contract award.

  Contractors should determine whether they can adequately insure for the risks of cyberattacks, and, if not, consider whether contracts entailing the management of sensitive data are too risky.

---

**Footnotes**

2 DFARS 252.246-7007 (containing 12 criteria that covered contractors must address to detect and avoid counterfeit electronic parts).
3 DFARS 252.246-7007(a).
4 Federal Acquisition Regulation (FAR) 52.203-13.
5 Metzger, Robert, You Don’t Have to Report Counterfeits to DOD IG, Law 360, October 9, 2014.
7 See U.S. Department of Defense, Report to Congress on FY 2013 Activities at the Defense Contract Audit Agency (March 24, 2014), available at http://www.dcaa.mil/DCAA_FY2013_Report_to_Congress.pdf (showing the percentage of examined costs that are questioned by DCAA to have more than tripled over the past decade, with a significant upward trend in the last several years. DCAA questioned 9.8 percent of costs examined in FY 2013, compared to 8.0 percent in FY 2012, 9.3 percent in FY 2011, and 6.0 percent in FY 2010). Id.
8 See Nadler, David, Chiarodo, Justin, and Zechmann, Stephanie, DCAA Access to Information—What You Need to Know and Strategies for Protecting Your Business, 56 The Government Contractor 30 (2014).
The LRN Ethics & Compliance Alliance (ECA) is an online community of thought leaders and practitioners that provides unique resources and support to enhance enterprise-wide knowledge, mitigate risk, support collaboration with experts, and implement program components. Encompassing practical and leading-edge resources, tools and content across 17 key ethics and compliance risk areas, the ECA is an invaluable partner resource for ethics and compliance program design, implementation and management strategies and provides important insights and tools to effectively mitigate and manage risk. Among other valuable subscriber benefits, the ECA provides a unique opportunity to interact and collaborate with leading subject-matter experts across all the major ethics and compliance risk areas and provides an extensive library of hands-on resources and tools to include model policies and program materials, risk assessment procedures, legal research, analyses of recent legal developments, and educational materials such as the ECA Risk Forecast Report.

The ECA Risk Forecast Report is an annual publication of the most significant risks facing organizations today, as reported upon and analyzed by 12 leading ethics and compliance experts. These individuals—leading specialists whose articles are featured in the body of the Report—provide insight into the regulatory and compliance challenges we face in 2015 and the developments that are likely to result.

NOTE: The specific focus area and expert perspective covered in this resource is an excerpt from our full ECA Risk Forecast Report and is representative of other major focus and risk areas covered and presented.

The full, 52-page Report is available on the LRN Ethics & Compliance Alliance (ECA) member site. If you are an ECA subscriber, please log onto the website to download the complete version. If you are not currently an ECA partner and would like to receive a copy of the full Report and learn more about our ECA Solution, please email us at ECA_Management@lrn.com.

The views and opinions expressed in the ECA Risk Forecast Report: (a) are for informational purposes only and are intended to represent only educated forecasts, not predictions of future events; and (b) are not presented for the purpose of providing legal advice. You should contact your legal counsel to obtain advice with respect to any particular legal or regulatory issue. In the case of opinions in this Report presented by a named author, those opinions are held by the individual author and do not necessarily reflect the opinions of that author’s employer or firm.
About LRN:
Inspiring Principled Performance

Since 1994, LRN has helped over 20 million people at more than 700 companies worldwide simultaneously navigate complex legal and regulatory environments and foster ethical cultures. LRN’s combination of practical tools, education, and strategic advice helps companies translate their values into concrete corporate practices and leadership behaviors that create sustainable competitive advantage. In partnership with LRN, companies need not choose between living principles and maximizing profits, or between enhancing reputation and growing revenue: all are a product of principled performance. LRN works with organizations in more than 100 countries and has offices in Los Angeles, New York, London, Mumbai, and Paris.

The LRN Ethics and Compliance Alliance (ECA) is a leading online solution that provides cutting-edge resources, tools, and practical content across all major ethics and compliance risk areas, including access to leading subject-matter experts for one-on-one collaboration and support.

For more information on this valuable solution, visit www.LRN.com/ethics-and-compliance-management-tools, email us at ECA_Management@lrn.com, or call: 800 529 6366 or 646 862 2040.

©Copyright LRN Corporation. All rights reserved.