SUMMER 2017
www.bdo.com

THE NEWSLETTER FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS: GOVERNMENT CONTRACTING

CLIENT Q&A: CHALLENGES GOVERNMENT CONTRACTORS FACE MAINTAINING A COMPLIANT SUPPLY CHAIN
PART FOUR

By Julia Bailey

Under the close eye of regulators, contractors are working against strong compliance headwinds as they expand their supply chains across international borders.

Effectively monitoring the supply chain from end to end and managing the risks associated with a complex network of suppliers and subcontractors is growing more onerous and time-consuming. To shed some light on where to focus your compliance efforts, we've developed a multi-part series to examine some of the key challenges contractors encounter when securing their supply chains.

In this final installment, we feature thoughts from our client, Julia Bailey, Compliance Counsel with professional services firm Jacobs, to examine export controls and anti-boycott laws and regulations as they pertain to government contractors' supply chains.

If you haven't already, check out:

- Part one here, for a look at the Contractor Purchasing System Review, recently released counterfeit parts rules and country of origin restrictions;

Ask the Pros

If you have a question—large or small—or are searching for a resource, you can count on our team to help you get on the right track with timely knowledge and thorough insights. Our practice combines extensive experience in government contracting work with deep understanding of the latest technical, compliance, accounting, regulatory and business matters important to contractors.

Go ahead, ask one of our pros.

CHRISTOPHER CARSON
National Government Contracting Practice Lead, Audit Partner
703-770-6324 / ccarson@bdo.com

ERIC SOBOTA
National Leader, Government Contracts and Grants Advisory Services
703-770-6395 / esobota@bdo.com

JOE BURKE
Partner, Transaction Advisory Services
703-770-6323 / jburke@bdo.com

STEPHEN RITCHEY
Audit Partner
703-770-6346 / sritchey@bdo.com

JEFF SCHRAGG
Tax Partner
703-770-6313 / jschragg@bdo.com

DEREK SHAW
Director
703-336-1501 / dshaw@bdo.com

ANDREA WILSON
Managing Director, Grants Advisory Services
703-752-2784 / aewilson@bdo.com

Read more ▶

CONTINUED FROM PAGE 1

A COMPLIANT SUPPLY CHAIN

- Part two here, for a thorough exploration of ethical considerations for government contractors, including the Federal Acquisition Register (FAR) "Contractor Code of Business Ethics and Conduct" clause, risk management for prime and subcontractor relations, the Combating Trafficking in Persons (CTIP) FAR clause and the False Claims Act (FCA).
- Part three here, for an examination of recent changes to the Foreign Corrupt Practices Act and the International Standards Organization anti-bribery management system.

Q: What are the most important export control requirements applicable to U.S. government contractors and their supply chains?

With more overseas contracting comes increased compliance risks associated with U.S. export control laws, namely the International Traffic in Arms Regulations (ITAR), 22 CFR 120-130, administered by the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) and the Export Administration Regulations (EAR), 15 CFR 730-774, administered by the Department of Commerce's Bureau of Industry and Security (BIS). Because exports are governed predominantly outside the Federal Acquisition Regulations (FAR), these regulatory requirements are often overlooked.

ITAR governs defense-related exports, while EAR governs dual-use exports as well as certain military items. An export includes: shipping items from the U.S., carrying controlled technical data out of the U.S. on an electronic device, transmitting controlled information electronically by any means, allowing access by "foreign persons" (as defined in the ITAR and EAR) to company computer networks with controlled technology and releasing controlled data during spoken conversations. The ITAR and EAR also control "re-exports or re-transfers," in which an item subject to U.S. jurisdiction is shipped or transmitted from one foreign country to another foreign country, or to an unauthorized user in the same foreign country.

Exports of "defense articles" (i.e., hardware, technical data and software) and "defense services" as defined and governed by ITAR are published in the U.S. Munitions List (USML). Exports of "dual-use technologies" (i.e., commodities, software or technology that have both commercial and military applications) are found on the Commerce Control List (CCL). Certain "defense articles" with purely military use are also found in the CCL in its Section 600 series.

Under ITAR, any item on the USML is controlled for exports to all countries, while an item subject to the EAR can be controlled for some countries, end users and end uses but not others (i.e., for closely allied countries). Under ITAR, to export, U.S. contractors must obtain export licenses or approval for exports, re-exports or re-transfers of items on the USML to every country in the world or to a foreign person. ITAR also obligates contractors to register with the DDTC (see DDTC Registration Guide). Under EAR, CCL-controlled exports may require a license for some countries, end users or end uses, or may be exported license-free or by using an applicable license to for closely allied countries. There are special, complex rules that apply to certain exports of encryption software and related technology or specific end uses, such as chemical and biological weapons.

Q: How should contractors look to manage their obligations under ITAR and EAR?

Contractors should not overlook ITAR and EAR requirements, as they are relevant at all stages of an opportunity. Neither ITAR nor EAR are incorporated directly into the FAR, except one DFARS provision at 225.7901 (and contract provision 252.225-7048) that specifies the need to comply with ITAR and EAR, and makes the failure to comply a possible contract violation.

Read more ▶

CONTINUED FROM PAGE 2

A COMPLIANT SUPPLY CHAIN

For ITAR-controlled technical data, foreign suppliers and subcontractors may need to enter into Technical Assistance Agreements, which are separate from their subcontracts and necessary to receive technical data and collaborate with U.S. entities higher up the supply chain.

For both ITAR- and EAR-controlled items, voluntary disclosures may be required in order to mitigate penalties and sanctions if a contractor believes its subcontractor has violated export control regulations (see **ITAR Part 127** and **EAR Part 764**). Contractors should consider including export control clauses in their subcontract agreements using the DFARS provision as a template. Such a contract clause should require the subcontractor to notify the contractor for any suspected export control violation and the contractor should preserve the right to conduct an export compliance audit of the subcontractor. Most importantly, because export controls compliance is a particularly complex area, contractors should seek outside advice, if possible. As an alternative, there are various resources available from **DDTC** and **BIS** for training company personnel.

Q: What should contractors be mindful of concerning anti-boycott laws and boycott requests from subcontractors or other third parties?

U.S. anti-boycott laws prohibit U.S. companies from cooperating with boycotts the U.S. does not support, including the Arab League boycott against Israel. While these regulations are often overlooked, compliance is complex and non-compliance can trigger stiff civil and criminal penalties, as well as loss of certain tax benefits. Anti-boycott laws are enforced by two regimes: The U.S. Department of Commerce's **Office of Anti-boycott Compliance (OAC)** and the **IRS**. Unfortunately, their rules are not consistent, meaning, among other things, practices that are punishable by one may not be punishable by the other and reporting requirements differ. For a summary of these differences, see the **Comparison of Commerce and Treasury Anti-Boycott Laws & Regulations/ Guidelines** published by the OAC.

There are three levels of an economic boycott: primary, secondary and tertiary. A primary boycott involves one country that refuses to trade with another country, such as the U.S.' former long-standing sanctions against Cuba. This type of boycott is not covered by OAC or IRS regulations. A secondary boycott is when one country refuses to trade with any party that does business with a country that is under a primary boycott. A tertiary boycott is when one country refuses to trade with any party that does business with companies or firms that are on their "blacklists." The OAC and IRS regulations prohibit secondary and tertiary boycotts.

A prohibited boycott request may come in the form of a certification, contract clause or any other communication, written or oral, received from government agencies, customers, distributors or other supply chain or business partners to take any action that has the effect of furthering or supporting a foreign boycott. Prohibited boycott requests include:

- To furnish information on business relations with Israel;
- To supply a negative statement or certification regarding the country of origin of goods;
- To give information about the race, religion, sex or national origin of another person;
- To do business only with approved firms or persons; or
- To require or insist on compliance with laws or regulations of a boycotting country, even if generally stated and whether there is a reference to boycott laws or regulations.

Contractors should ensure that employees and subcontractors are trained to identify a boycott request, review commercial documents or communications closely to identify boycott issues, avoid carrying out a boycott request and know where to direct such requests for further instruction. If a contract is governed by DFARS and includes DFARS 252.225-7031, a "foreign offeror," as defined in the regulation, will have to certify that it does not comply with the Secondary Arab Boycott of Israel. Contractors should include in subcontracts a requirement that subcontractors comply with anti-boycott laws.

Contractors and subcontractors will be required to report quarterly to the OAC and annually to the IRS the requests they have received since the previous reporting period. Any failure to comply with anti-boycott regulations or to report a boycott request should be disclosed through the voluntary self-disclosure procedure of each agency. For the OAC, contractors should follow the procedures in EAR 764.8. As tensions persist in the Middle East, contractors will need to remain watchful for potential boycott requests from Arab League countries, some of which are home to critical suppliers for American commercial companies and contractors.

Julia Bailey joins BDO as a guest author. She may be reached at jkbaileydc@gmail.com.

Read more ▶

UNDERSTANDING NEW CYBER AND IT-ORIENTED REGULATIONS FOR CONTRACTORS

By Karen Schuler and Derrick King

Following widespread cyber attacks like the May WannaCry and more recent Petya ransomware attack that included thousands of ransomware attacks across the globe, protecting against cybersecurity is top of mind in Washington, D.C., and beyond.

In efforts to keep sensitive information as secure as possible, government contractors will be held to similar standards to that of the federal government as outlined in The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171. NIST SP 800-171 provides guidelines for companies to control the security of Controlled Unclassified Information (CUI). This requirement will be imposed government-wide in 2017 via the final Federal Acquisition Regulation (FAR) rule, an expansion of the current Defense Federal Acquisition Regulation Supplement (DFARS) implemented in June 2016—meaning now's the time to understand how the rule impacts your organization and how you may need to shore up your controls to stay compliant.

NIST SP 800-171 ensures CUI and Department of Defense (DOD) Covered Defense information in non-federal systems and organizations are protected accordingly. CUI is a result of Executive Order 13556, issued on Nov. 4, 2010. The CUI system aims to standardize and simplify how the executive branch of the government handles unclassified information that requires safeguarding or dissemination controls consistent with applicable law, regulations and government-wide policies. There are 22 approved CUI categories covering everything from agriculture to geodetic product information, transportation and everything in between, including documents like drawings and specifications provided by the government.

Both the FAR and DFARS explicitly state that federal contractors must comply with 14 cybersecurity controls to protect their information systems. Of those 14 cybersecurity controls within NIST SP 800-171, seven may be of unique interest to non-federal entities and require additional explanation:

- Access Control
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Physical Protection
- Awareness and Training

According to NIST, there are two classifications of security requirements: basic and derived. The basic security requirements are obtained from Federal Information Processing Standard Publication 200 (FIPS 200), which provides the high-level and fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53.

Read more ▶

CONTINUED FROM PAGE 4

CYBER AND IT-ORIENTED REGULATIONS

ACCESS CONTROL

Basic security requirements for access control include limiting information system access and processes to authorized users or devices. Contractors should limit information system access to the types of transactions and functions that authorized users are allowed to execute.

There are 19 derived security requirements. Examples include encrypting CUI on mobile devices, employing the principle of least privilege—including for specific security functions and auditing the execution of such functions—like limiting unsuccessful login attempts.

IDENTIFICATION AND AUTHENTICATION

For identification and authentication, basic security requirements include identifying information system users and processes acting on behalf of users or devices. Contractors are also required to authenticate, or verify, the identities of those users, processes or devices before allowing access to organizational information systems.

Contractors also are required to enforce a number of derived security requirements, including storing and transmitting only encrypted representations of passwords, preventing reuse of identifiers for a defined period and disabling identifiers after a defined period of inactivity, among others.

INCIDENT RESPONSE

Basic and derived security requirements for incident response are minimal. A contractor must establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities. Additionally, they are also required to track, document and report incidents to appropriate officials and/or internal and external authorities. Finally, the contractor should test the organizational incident response capability in case of an emergency.

MEDIA PROTECTION

To ensure media protection, contractors are required to physically protect information system media containing CUI. This includes limiting access to CUI on information system media for authorized users and sanitizing or destroying information system media containing CUI before disposal or release for reuse.

Derived security requirements outline, among other things, that a contractor must mark media with necessary CUI markings and distribution limitations, control the use of removable media on information system components, and implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport, unless otherwise protected by alternative physical safeguards.

PERSONNEL SECURITY

While there are no derived security requirements for personnel security, at a basic level, contractors should screen individuals before authorizing access to information systems containing CUI. They should also ensure CUI and information systems containing CUI are protected during and after personnel changes like terminations and transfers.

PHYSICAL PROTECTION

According to NIST, basic requirements for physical protection require limiting physical access to organizational information systems, equipment and the respective operating environments to only authorized individuals. Infrastructure for those information systems should be protected, monitored and supported at all times.

Derived security requirements mandate escorting and monitoring visitors, keeping audit logs of physical access, enforcing safeguarding measures for CUI at alternative worksites, and controlling and managing access to physical devices.

AWARENESS AND TRAINING

To ensure proper awareness and training, contractors should confirm all users of organizational information systems are aware of security risks associated with their activities and applicable policies, standards and procedures related to the security of organizational information systems. Contractors should also ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. NIST requirements also mandate that contractors provide security awareness training on recognizing and reporting potential indicators of insider threats.

To make sure you're prepared for the government-wide implementation of the basic and derived security requirements, begin planning now to ensure compliance. Conduct a gap analysis to understand what needs to be done to meet the requirements and prevent lost business due to non-compliance. There is no one-size-fits-all approach to compliance—make sure your plan reflects your organization's unique DNA before it's too late.

Karen Schuler is a partner and National Information Governance Practice Leader and can be reached at kschuler@bdo.com.

Derrick King is a senior manager and can be reached at dking@bdo.com.

Read more ▶

IN AN UNCERTAIN TIME, CONSIDER ESOPS

By Jay Powers

In an uncertain time for government budgets and priorities, government contractors may consider implementing Employee Stock Ownership Plans (ESOP) as a smart way to reward company stakeholders and encourage cash flow.

An ESOP is a qualified, defined contribution employee benefit plan, much like a traditional profit-sharing plan that invests primarily in the sponsoring employer's stock. They are unique among qualified benefit plans because the ability to borrow money may be used as a technique of corporate finance.

There are approximately 10,000 ESOPs in place in the U.S., covering 11 million employees, or 10 percent of the private sector workforce. Most of these companies have other retirement plans, such as defined benefit pension plans, or 401(k) plans, to supplement their ESOP. About 800 ESOPs are in place at publicly traded companies.

Tax advantages of Implementing ESOPs

While there are many benefits to implementing ESOPs, like fluidity and independence, it's important not to overlook the tax advantages to government contractors:

Deductibility of Principal and Interest Payments

Principal and interest payments of an ESOP loan are considered contributions to a tax-qualified employee benefit plan and thus are tax deductible. For an S corporation, the maximum deductible amount is 25 percent of covered eligible payroll and—unlike a C corporation—both principal and interest are included in the 25 percent limit. However, an ESOP is a non-tax-paying shareholder, so an S corporation that is owned fully by an ESOP should not pay any federal income tax and could avoid state income tax.

Deductibility of Dividends

In a C corporation, dividends paid on stock held by the ESOP are tax deductible to the corporation if they are distributed to the ESOP, and do not count toward the 25 percent limit on principal and interest deductibility. Thus, these dividends may be used to pay additional principal and interest on the ESOP loan. It's important to note, however, that dividends are not deductible for S corporation ESOPs.

ESOP Rollover

Shareholders selling to a C corporation may leverage ESOPs to qualify to defer capital gains taxes on the gain from the sale by purchasing "qualified replacement securities" with the proceeds from the sale.

Step-Up in Cost Basis to Seller's Estate

Should a selling shareholder "roll over" assets in a IRC §1042 transaction, the estate could receive a step-up in cost basis on the qualified replacement securities at death, thus eliminating the capital gains tax liability.

Transitioning to an ESOP presents government contractors with flexibility and benefits that may be advantageous in the current industry climate.

Jay Powers is the National Practice Leader for BDO's ESOP Transaction Services and may be reached at jpowers@bdo.com.

Read more ▶

ANOTHER YEAR IN THE BOOKS: DCAA'S FY 2016 REPORT TO CONGRESS

By Giacomo Apadula

The Defense Contract Audit Agency (DCAA) recently issued its sixth annual report to Congress on March 31, 2017 (the Report). DCAA primarily provides audit and financial advisory services to the Department of Defense (DOD) and has been ordered by Congress to issue an annual report.

The report must address significant problems/deficiencies encountered during audits, statistics on audit performance during the previous fiscal year and a summary of recommendations to improve the audit process. The FY 2016 report highlights DCAA's activity, its successes in FY 2016 and thoughts and predictions about FY 2017.

Here are the key takeaways from the latest report and our thoughts on how the contracting community may be impacted.

ORGANIZATIONAL STRUCTURE AND STAFFING

What it says: Since its inception in 1965, DCAA has been organized by geographic regions allowing them to be close to the contractors they audit. However, DCAA noted that major defense contractors have steadily decentralized operations and increased office locations in the U.S. and worldwide. Over this time span, multiple DCAA regions have held jurisdiction over different audits for a single contractor, increasing the likelihood of inefficiencies in operations and communication.

After the recent success of its pilot program to geographically consolidate disbursed audit teams, DCAA has decided to realign its organizational structure into four Corporate Audit Directorates and three geographical regions, with a field detachment office focused on classified work (effective October 2016). The Corporate Audit Directorates are organized by major contractors, while the three geographic regions are primarily focused on small and mid-sized contractors.

What it means: Large defense contractors will be brought under an executive team that provides one point of contact for all DCAA matters related to each contractor and its business. DCAA hopes this leads to improved efficiency and effectiveness, reduced redundancy and better customer service by centralizing internal support functions. DCAA also hopes for greater consistency in the implementation of policy and audit practices within the respective directorates

Read more ▶

CONTINUED FROM PAGE 7

DCAA'S FY 2016 REPORT TO CONGRESS

and regions. It is expected to take some time for Corporate Audit Directorates and Regional Audit Managers to realign their priorities within their respective companies and geographies, leading to potential delays in routine audit practices.

What we think: Only time will tell if this reorganization will help DCAA address its efficiency concerns. It theoretically bodes well for contractors. That said, meaningful change takes time. DCAA is already prefacing these changes with an expectation for "delays in routine audit practices" – meaning the desired changes won't happen overnight. Contractors should look for ways to strengthen and/or re-engage relationships with their DCAA points of contact and establish audit expectations early in the process.

FY 2016 AUDIT PERFORMANCE

What it says: According to the report, the DCAA examined nearly $287 billion in FY 2016 across 4,269 audit reports issued. This increase—nearly $29 billion over FY 2015—was largely due to the DCAA setting its priorities to higher-risk areas and higher-dollar audits (a risk-based approach). This helped generate net savings of $3.6 billion in FY 2016, a $500 million increase over FY 2015. The DCAA returned $5.70 for each dollar invested, an increase of 90 cents from FY 2015. These increases in net savings and ROI were driven by greater sustention rates in forward-pricing-rate proposal audits and higher dollars associated with the audits. The report goes into detail behind these numbers and specifically addresses the incurred cost backlog, questioned costs sustained and completed audit reports.

Incurred cost (IC) audits remained DCAA's top priority in FY 2016, totaling 2,103 of 4,269 audits. On average, IC audits took 138 days to complete. IC audits were followed by 981 special audits (e.g., typically those in response to requests from contracting officers for an independent financial opinion on elements of a contract or on a contractor's accounting business system) took an average of 133 days to complete. A total of 873 forward-pricing audit reports were completed in FY 2016, averaging 86 days to complete. Other audits made up 312 of the 4,269 audit reports completed in FY 2016. These primarily included compliance with cost accounting standards, review of contractor business systems and contractor compliance with TINA.

QUESTIONED COST SUSTAINED (BILLIONS)

	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016
Question Costs	$ 8.5	$ 9.6	$ 12.3	$ 11.7	$ 9.0
Questioned Cost Sustained	$ 4.5	$ 5.1	$ 5.7	$ 5.9	$ 4.7
Percent Sustained	**52.2%**	**52.8%**	**46.4%**	**50.6%**	**52.5%**

Incurred Cost

One of DCAA's ongoing priorities is to eliminate its incurred cost backlog. A dedicated team was established in FY 2012 to focus entirely on this effort. Despite this, the DCAA only closed 8,100 incurred cost years in FY 2016, compared to 9,400 in FY 2015. However, in FY 2016, the DCAA met its goal set by the National Defense Authorization Act to reduce the incurred cost backlog to within 18 months. To accomplish this, all non-DOD entity audits were stopped until the DCAA realized the goal (which it did in September 2016). With the incurred cost backlog at 4,677 submissions at the end of FY 2016, the DCAA could see its elimination soon and set the goal for March 2018. Unfortunately, the DCAA is already facing hurdles to keep up FY 2016 numbers in FY 2017.

What it means: The DCAA's cost recovery efforts have been considerably slowed and, in many cases, stalled for the government while industry is finding itself with a weighty burden of maintaining records for a growing number of matters for longer periods. Reaching the threshold to take on non-DOD audits could lead to a bigger backlog. The less time the agency has to spend on incurred costs audits, the more issues will arise in other areas further down the road. Thus, DCAA will do as it did in FY 2016 and prioritize the highest payback audits, forward pricing and incurred cost. Its goal to perform accounting system, estimating system and MMAS audits may get off the ground, but it may not pick up much speed. It is still questionable whether or to what extent the DCAA will continue to involve itself with non-audit support activities. There are compelling reasons that the DCAA should focus only on auditing DOD-incurred cost proposals, or at least until they have completely eliminated the backlog.

What we think: The battle against the backlog is real and will continue to impact contractors as contract funds expire and indirect rates remain unsettled. We expect DCAA to continue to raise the bar for Incurred Cost Proposal (ICP) "adequacy" determinations.

Additionally, as more DCAA resources remain focused on the incurred cost issue, the backlog could grow in others areas (i.e., business systems). Overall, we expect the timeliness of audits to remain a challenge for the foreseeable future.

Questioned Costs Sustained

In FY 2016, $4.7 billion of $9.0 billion questioned costs were sustained, or 52.5 percent. This number is an increase over the previous two years, largely due to improved engagement with contracting officers. The table above compares questioned costs and sustention rates for fiscal years 2012-2016.

Read more ▶

CONTINUED FROM PAGE 8

DCAA'S FY 2016 REPORT TO CONGRESS

What it means: DCAA only correctly identifies questioned costs half the time—they are not correct the other 50 percent of the time.

What we think: Our hope is that DCAA will devote resources to increasing its sustention rate for questioned costs and strengthening its methodology for questioning costs.

RECOMMENDED ACTIONS OR RESOURCES TO IMPROVE THE AUDIT PROCESS

What it says: The report identifies contract auditing as a critical step in the government's acquisition process and determines DCAA's independent opinion directly affects the value that the government, tax payer and warfighter receive. DCAA suggests two ways to help prevent potential acquisition disruptions and improve the audit process efficiencies:

- Early DCAA engagement on congressional proposals; and
- Assistance in maintaining a steady staffing level.

Additionally, DCAA looks to ensure Congress has critical information when developing proposals and making decisions. The DCAA's inconsistent staffing has been a thorn in its side. The DCAA wants the budget to maintain staffing at 5,100 employees. This is a 600-employee increase from its current level of 4,524, the lowest since FY 2009.

What it means: DCAA is seeking more authority and manpower to carry out its mandate.

What we think: How DCAA would fare with earlier engagement in the congressional proposal process is unclear. Without the manpower to overcome the audit backlog, gathering, analyzing and communicating such information to Congress in a timely enough manner to produce meaningful input is a tall order.

BUSINESS SYSTEM INITIATIVE

What it says: DCAA is responsible for auditing three of the six major business systems: Accounting, Estimating, and Material Management and Accounting. With the focus of its limited resources primarily on high-risk forward pricing and incurred cost audits, few business system audits had been completed in FY 2016.

As such, in FY 2017, DCAA is investigating ways to leverage internal audit work performed by the contractor without violating standards. One initiative includes using Textron Corporation's internal group to perform certain portions of field work. In another initiative, DCAA is asking contractors to submit working papers from the Sarbanes-Oxley testing performed as part of its financial statement audit and other internal accounting system audits.

What it means: In FY 2017, the DCAA plans to commit resources to audit high-risk Estimating Systems and Material Management and Accounting Systems (MMAS), starting with fully tested audit programs published in early FY 2017. If the DCAA is able to get current on incurred cost audits, taking business system audits to a larger scale can help make the relationship between DCAA and industry more efficient, assuming industry is prepared for the event. However, DCAA's intent to leverage existing internal audit workpapers may expose contractors to more risk for DCAA auditor interpretation.

What we think: Leveraging internal audits contractors are already performing sounds like a great way to lessen the burden of dealing with DCAA audits. But contractors should be wary. DCAA could require all government contractors to maintain a robust internal audit function. Leveraging such workpapers may result in DCAA expanding its audit procedures—not lessening.

CONCLUSION

With another year in the books and another DCAA report to Congress, what did we learn?

- A re-organization/streamlining of DCAA is coming. Contractors should be prepared for delays in routine audit work, but look for opportunities to strengthen relationships with DCAA and establish audit expectations early in this process;
- DCAA continues to focus on incurred cost audits, and while the backlog dwindled, the recent hiring freeze has forced DCAA to reassess its elimination goal of March 2018;
- DCAA suggests Congress give it more authority and manpower to complete its objective, and
- DCAA is exploring ways to leverage internal audit workpapers to support business system audits. Contractors should take heed.

We look forward to seeing how the year ahead progresses.

Parker Wolfinger, Senior Associate, contributed to this article.

Giacomo Apadula is a Managing Director and can be reached at gapadula@bdo.com.

Read more ▶

QUARTERLY REGULATORY UPDATE

FINAL FAR

EXECUTIVE COMPENSATION THROUGH TOTAL SHAREHOLDER RETURN FOUND UNALLOWABLE; ASBCA NO. 58966, APPEAL OF EXELIS INC.

KEY DETAILS: The appellant's executive compensation model included total shareholder returns, calculated using unallowable variables and therefore expressly unallowable. The contracting officer properly applied a penalty for submitting a final indirect cost rate proposal including expressly unallowable costs.

EFFECTIVE: April 21, 2017

FINAL RULE – UNIFORM ADMINISTRATIVE REQUIREMENTS, COST PRINCIPLES, AND AUDIT REQUIREMENTS FOR FEDERAL AWARDS

KEY DETAILS: The Office of Management and Budget (OMB) is updating the final guidance that appeared in the Federal Register on December 26, 2013. Guidance on the effective/applicability date is revised to allow a grace period of one additional fiscal year for non-Federal entities to implement changes to their procurement policies and procedures in accordance with guidance on procurement standards. Other requirements in the section remain unchanged. For all non-Federal entities, there is an additional one-year grace period for implementation of the procurement standards in 2 CFR 200.317 through 200.326. This means the grace period for non-Federal entities extends through December 25, 2017, and the implementation date for the procurement standards will start for fiscal years beginning on or after December 26, 2017.

EFFECTIVE: May 17, 2017

FINAL DFARS

AGENCY CAN REASONABLY CONCLUDE TECHNICAL APPROACH HAS MERIT, WHILE REJECTING PROPOSED COST SAVINGS

KEY DETAILS: Glacier Technical Solutions LLC protested the Army's award of a contract for test and evaluation technical services to SAWTST LLC. The Army had rejected SAWTST's proposed cost savings, but merited a good rating for its technical approach. Glacier argued that the Army could not reasonably reject the cost savings associated with a proposed staffing methodology without rejecting the technical efficacy of that staffing methodology itself, but GAO disagreed. The GAO argued that there is nothing to prohibit the Army from approving the technical approach, while also making an upward cost adjustment to account for any existing concerns.

EFFECTIVE: March 28, 2017

PROPOSED RULES – AGENCY SUPPLEMENTS TO THE FAR

HOUSE BILL WOULD LIMIT CREDIT FOR SMALL BUSINESSES FALLING INTO MULTIPLE SOCIOECONOMIC CATEGORIES

KEY DETAILS: Legislation introduced in the House would amend the Small Business Act to limit the way agencies receive credit for contracting with small businesses in several socioeconomic categories. The Assuring Contracting Equity Act of 2017 would limit the number of categories for which a small business may qualify in order to prevent an agency from taking credit for an award in more

Read more ▶

CONTINUED FROM PAGE 10

REGULATORY UPDATES

than two specified small business categories. The bill also would prevent an agency that contracts with an 8(a) small business from taking credit for that award under any category other than small disadvantaged business. Agencies currently can take credit for an award under all categories for which a vendor qualifies. The bill also would increase the government-wide small business prime contracting goal from 23 to 25 percent, the goals for prime and subcontract awards to small businesses owned and controlled by socially and economically disadvantaged individuals and to WOSBs from 5 to 10 percent, and the goals for prime and subcontract awards to SDVOSBs and HUBZone concerns from 3 to 6 percent.

EFFECTIVE: May 31, 2017

SMALL BUSINESS SIZE STANDARDS; ADOPTION OF 2017 NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM FOR SIZE STANDARDS

KEY DETAILS: The U.S. Small Business Administration (SBA) proposes to amend its small business size regulations to incorporate the U.S. Office of Management and Budget's (OMB) North American Industry Classification System (NAICS) revision for 2017, identified as NAICS 2017, into its table of small business size standards. NAICS 2017 created 21 new industries by reclassifying, combining, or splitting 29 existing industries under changes made to NAICS in 2012. SBA's proposed size standards for these 21 new industries have resulted in an increase to size standards for six NAICS 2012 industries and part of one industry, a decrease to size standards for two, a change in the size standards measure from average annual receipts to number of employees for one, and no change in size standards for 20 industries and part of one industry. SBA proposes to adopt the updated table of size standards.

EFFECTIVE: April 18, 2017

FINAL RULES – AGENCY SUPPLEMENTS TO THE FAR

2017 NDAA'S IMPACT ON AUDITS AND COST ACCOUNTING STANDARDS

KEY DETAILS: Section 820 of the National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-238, 130 Stat. 2000 (NDAA), makes three significant changes to the federal government's future use of cost accounting standards (CAS). First, it empowers contractors to avoid Defense Contract Audit Agency (DCAA) audits by employing private auditors to audit their rates. Section 820(b)(1) of the NDAA authorizes defense contractors to present commercial auditors' findings to the DCAA, which must accept them without performing additional audits so long as indirect costs were audited and the commercial auditor used a relevant accounting standard, e.g., Generally Accepted Accounting Principles (GAAP). This development could be of great significance, and may enable contractors to accelerate the audit process and reduce the risk of protracted and inaccurate audits performed by the DCAA. Next, it creates a new and independent Defense Cost Accounting Standards (DCAS) Board to oversee cost accounting standards across the Department of Defense (DoD). The newly-created Defense Cost Accounting Standards (DCAS) Board will ensure "uniformity and consistency in the standards governing defense contracts." The DCAS Board will have three primary duties: 1) reviewing cost accounting standards created by, and recommending changes to, the CAS Board; 2) implementing cost accounting standards across the DoD; and 3) developing standards to ensure DoD's adherence to standards established by the CAS Board or GAAP. Finally, the FY17 NDAA provides direction to the federal government's existing CAS Board. Although § 820 is titled "Defense Cost Accounting Standards," its first order of business is to amend the existing CAS Board's implementing statute, 41 U.S.C. § 1501. Id. at § 820(a). Specifically, it directs the CAS Board to meet at least once per quarter, publish notice of each meeting and the meeting's agenda in the Federal Register, and report annually to multiple congressional committees regarding how it has conformed its accounting standards to GAAP and minimized the burden on contractors. Moreover, the CAS Board is directed to "ensure that the cost accounting standards used by Federal contractors rely, to the maximum extent practicable, on commercial standards and accounting practices and systems." Finally, the minimum value of waiver-eligible contracts is increased from $15 million to $100 million, id. at § 820(a)(2), meaning agency heads may waive the CAS Board's and, presumably, DCAS Board's standards for contracts valued at less than $100 million.

EFFECTIVE: March 8, 2017

CONTRACTOR'S ACCOUNTING OF BUILDING LEASE COSTS NOT A VIOLATION OF CAS 404; ASBCA 60131, APPEAL OF EXELIS INC.

KEY DETAILS: The government's request for reconsideration of the partial dismissal of a government claim due to noncompliant accounting for the costs of a building lease is denied, where the contractor did not consider its leased assets a capital lease, and therefore any errors in reporting its lease costs were not a violation of Cost Accounting Standard 404.

EFFECTIVE: March 22, 2017

GAO RECOMMENDS REIMBURSEMENT OF COSTS PROTESTING AGENCY'S BEST-VALUE TRADEOFF DECISION, WHICH WERE INTERTWINED WITH MERITORIOUS CHALLENGES TO EVALUATION OF EXPERIENCE AND PAST PERFORMANCE; GAO B-413116.38, CHAGS HEALTH INFORMATION TECHNOLOGY LLC, ET AL—COSTS

KEY DETAILS: Multiple requests that GAO recommend the agency reimburse the protesters' reasonable costs of pursing their protests of the agency award decision are denied in part, where the protest grounds were clearly severable from arguments the agency

Read more ▶

CONTINUED FROM PAGE 11

REGULATORY UPDATES

conceded were reasonable, and were not clearly meritorious, and sustained in part, where GAO concluded that challenges to the agency's best-value trade-off decision were not severable from the clearly meritorious protests challenging the agency's evaluation of corporate experience and past performance, because the best-value tradeoff decision relied heavily on portions of the evaluation the agency conceded were flawed.

EFFECTIVE: May 3, 2017

GOVERNMENT-CAUSED DELIVERY DELAYS MAY HAVE BREACHED IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING; CAFC NO. 2016-1265, AGILITY PUBLIC WAREHOUSING CO. KSCP V. JAMES N. MATTIS, SECRETARY OF DEFENSE

KEY DETAILS: A contract modification provided that the government would consider claims based on government-caused delivery delays but did not guarantee they would be paid. However, the Armed Services Board of Contract Appeals failed to properly consider whether the government had breached its implied duty of good faith and fair dealing by engaging in conduct that prevented the appellant from making its deliveries in a timely manner. The Board also failed to consider whether the government had constructively changed the contract by its conduct.

EFFECTIVE: April 20, 2017

GOOGLE'S MOTION TO DISMISS IN THE MATTER OF OFFICE OF FEDERAL CONTRACT COMPLIANCE PROGRAMS, U.S. DEPARTMENT OF LABOR V. GOOGLE INC., WAS DENIED

KEY DETAILS: After a compliance review for potential wage discrimination, the US DOL made comments to the press that Google had committed violations upon its award of a GSA contract. Based on a published article where DOL made comments about its determination on Google's review, Google contended that the US DOL had completed its review and that Google's was required to provide additional information and that the case should be dismissed. Although concluding comments were made by the US DOL, Google's motion to dismiss was denied.

EFFECTIVE: May 2, 2017

EXECUTIVE ORDERS

PRESIDENTIAL EXECUTIVE ORDER ON STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

KEY DETAILS: President Trump signed the long-awaited EO on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" on May 11, the objective of which is to improve network security of U.S. Government agencies, enhance protection of national infrastructure, and develop a more robust cyber deterrence strategy. The related press release, released by the Office of the Press Secretary on May 11, 2017, cites the following as methods of achieving this objective:

Agency heads have been directed to immediately use the National Institute of Standards and Technology (NIST) Cybersecurity Framework for risk management, and to provide within 90 days a risk management report to DHS and the Office of Management and Budget (OMB) on the implementation of the framework and risk management strategies employed by the department or agency.

DHS and OMB have been directed to assess federal agencies' cybersecurity risk management strategies in order to determine the adequacy of cyber protections across federal networks and identify any unmet budgetary or policy needs.

DHS and OMB are to provide a plan to the president, within 60 days of receiving the agency reports, on how to protect the executive branch enterprise.

DHS and other agencies are to provide the president with a report within 90 days on the technical feasibility to transition all agencies to one or more consolidated network architectures and shared IT services.

RELEASE: May 11, 2017

PRESIDENTIAL EXECUTIVE ORDER ON IDENTIFYING AND REDUCING TAX REGULATORY BURDENS

KEY DETAILS: President Trump's executive order states that "immediate action is necessary to reduce the burden existing tax regulations impose on American taxpayers and thereby to provide tax relief and useful, simplified tax guidance." This action is intended to alleviate the impact of regulations that have "increased tax burdens, impeded economic growth, and saddled American businesses with onerous fines, complicated forms, and frustration."

RELEASE: April 21, 2017

WHITE HOUSE SAYS DOD CONTRACTS SHOULD BE FIXED-PRICE

KEY DETAILS: In a recent interview in *Time* magazine, the president expressed his preference for the use of fixed-price contracts for Department of Defense programs, and suggested future military contracts could be renegotiated to ensure they have fixed prices.

RELEASE: May 11, 2017

Read more ▶

SIGNIFICANT ACCOUNTING & REPORTING UPDATES

The FASB recently issued ASU 2017-09, Scope of Modification Accounting, to clarify which changes to the terms or conditions of a share-based payment award require an entity to apply modification accounting in Topic 718, Stock Compensation. The ASU is available here, and becomes effective for all entities for fiscal years beginning after Dec. 15, 2017.

Topic 718 provides an accounting framework applicable to modifications of share-based payments, and currently defines a modification as "a change in any of the terms or conditions of a share-based payment award." This definition is open to a broad range of interpretation and has resulted in diversity in practice as to whether certain changes in terms or conditions are treated as modifications.

ASU 2017-09 clarifies that an entity must apply modification accounting to changes in the terms or conditions of a share-based payment award unless all of the following criteria are met:

1. The fair value of the modified award is the same as the fair value of the original award immediately before the modification. The standard indicates that if the modification does not affect any of the inputs to the valuation technique used to value the award, the entity is not required to estimate the value immediately before and after the modification.
2. The vesting conditions of the modified award are the same as the vesting conditions of the original award immediately before the modification.
3. The classification of the modified award as an equity instrument or a liability instrument is the same as the classification of the original award immediately before the modification.

The ASU also clarifies that the disclosure requirements in paragraphs 718-10-50-1 through 50-2A and 718-10-50-4 apply regardless of whether an entity is required to apply modification accounting. If applicable, this includes disclosing a lack of incremental compensation cost resulting from a modification.

In addition, the ASU includes examples of common changes to the terms or conditions of an award and indicates whether those changes typically require an entity to apply modification accounting.

Examples of changes to an award that generally do not require modification accounting:

- Changes that are administrative in nature, such as a change to the company name, company address or plan name
- Changes in an award's net settlement provisions related to tax withholdings that do not affect the classification of the award

Examples of changes to an award that generally require modification accounting include:

- Repricing of share options that results in a change in value of those share options
- Changes in a service condition
- Changes in a performance condition or a market condition
- Changes in an award that result in a reclassification of the award (equity to liability or vice versa)
- Adding an involuntary termination provision in anticipation of a sale of a business unit that accelerates vesting of the award

DID YOU KNOW...

Washington Technology's Contractor Confidence Index experienced a post-election bump, rising to 113.3 in Q1 2017, 15 points higher than the previous index from August 2016.

The largest five federal contractors had a combined $90.6 billion in obligations in FY15, according to Bloomberg Government's BGOV200 ranking of the top federal contractors based on prime contracts.

According to BDO's 2017 Manufacturing RiskFactor Report, 37 percent of the largest public U.S. manufacturers cite loss of government contracts, spending or incentives as a risk in their latest SEC filings.

Federal grants to state and local government and territories totaled $624 billion for FY15, according to USAfacts.org data on government spending.

In March, the U.S. Army sent a solicitation for information on prototyping efforts for robotic vehicles, hoping to have a prototyping project complete by FY22, according to National Defense.

Read more ▶

PErspective in GOVERNMENT CONTRACTING

A FEATURE EXAMINING THE ROLE OF PRIVATE EQUITY IN THE GOVERNMENT CONTRACTING SPACE.

Despite major budget cuts, proposed legislative shifts and unfilled federal government positions, the outlook for government contractors has been optimistic. Earlier this year, private equity activity for the government contracting industry was looking up. According to a Washington Technology report, a post-Trump bump boosted sector valuations, averaging 11x forward earnings before interest, tax, depreciation and amortization (EBITDA).

Today, the mood in Washington remains positive as contractors—especially in the aerospace and defense industries—predict growth, federal government spending and budgets will be in their favor. According to Bloomberg Government, many contractors who were taking a "wait and see" attitude prior to the November elections are now leaning into an "invest and grow" mentality in areas like infrastructure and technology.

As contractors are actively investing more in technology, expect strategic IT deals to play a major role in the year ahead. We've already seen top contractors making big moves in the deal space this year. Lockheed Martin recently divested its Information Systems & Global Services business to Leidos, which resulted in Lockheed slipping from number one in Washington Technology's Top 100 to number two. Leidos assumed the top spot post-transaction.

Companies lower on Washington Technology's list are also making moves in cyber, IT and cloud technologies through strategic hires and partnerships. Other notable deals in the space this year include the merger of HPE's enterprise services business with Computer Sciences Corp. to create DXC Technology. DXC will aim to "modernize and digitize outdated government processes."

We continue to see many large and mid-sized government contractors consider carving out non-strategic business lines. Their boards and senior leaders are reassessing their portfolio of capabilities and customers to focus the company's resources on areas of expertise and growth. Financial buyers and smaller government contractors have shown great interest in these discarded businesses as they possess or have access to senior leadership to run the carve-outs though are keen to fully understand the stand-alone abilities of the carve-out businesses and the areas of investments needed.

Overall, we are currently experiencing a seller's market for government contracting M&A. Investment bankers are very active with robust auctions for small and mid-sized government contractors with unrestricted contracts and a healthy pipeline to capture higher valuations. While we are seeing smaller government contractors with set-aside revenue completing transactions, the market of buyers for these businesses is shrinking as buyers see the risk of the set-aside work not continuing post-transaction, which then produces a lower valuation, or no transaction at all.

Sources: Washington Technology, Bloomberg Government

Read more ▶

MARK YOUR CALENDAR...

AUGUST

Aug. 21-25
Focused Government Contract Costs and Accounting Training
Waterview Conference Center
Arlington, Va.

Aug. 24-25
Earned Value Management Practitioners' Training and Symposium
Waterview Conference Center
Arlington, Va.

SEPTEMBER

Sept. 12
Prevailing Wage Seminar*
Location and registration TBD

Sept. 13
Cyber Insurance Seminar*
Location and registration TBD

Sept. 14
Revenue Recognition Event*
Location and registration TBD

OCTOBER

Oct. 10-11
2017 Government Contract Financial Management Review & Outlook
Hyatt Regency Crystal City
Arlington, Va.

Oct. 23-26
Deltek Insight*
Gaylord Opryland Resort & Convention Center
Nashville, Tenn.

** indicates BDO is hosting or attending this event*

People who know Government Contracting, know BDO.