SUMMER 2015
www.bdo.com

THE NEWSLETTER FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS: GOVERNMENT CONTRACTING

Speaking: Robert Craig, GCAS Managing Director, BDO; *Left to right:* Nick Sanders, President, Apogee Consulting; Steve Trautwein, Acting Director, DCMA Cost & Pricing Center; Matt Popham, VP, Government Compliance Director, Leidos

IN CASE YOU MISSED IT: SECOND ANNUAL BDO EXECUTIVE SEMINAR FOR GOVERNMENT CONTRACTORS

On April 28, nearly 300 professionals across the government contracting industry gathered at BDO's 2015 Executive Seminar for Government Contractors – 100 more attendees than last year – to discuss a number of issues affecting today's contracting marketplace.

Among the day's speakers were Virginia Congresswoman Barbara Comstock, as well as other leading industry professionals. Co-hosted with law firm BakerHostetler and the Public Contracting Institute, the event covered a wide range of issues pertinent to contractors, including the current DCAA/DCMA environment, compliance matters, the impact of business systems requirements in today's marketplace and the latest legal updates.

There were several overarching themes that emerged from the day's panels and discussions, including:

UNCERTAINTY PREVAILS IN THE GOVERNMENT CONTRACTING INDUSTRY

Speakers addressed defense cutbacks, sequestration and mounting challenges surrounding the lowest price technically acceptable (LPTA) method of evaluating contracts. Budget uncertainty has added a new strain on the relationships between government regulators and contractors, contributing to the growing popularity

DID YOU KNOW...

According to *Washington Technology's* ***Insider Report***, slightly more than half of government contractors said they expected they would continue to use subcontractors at a consistent rate, and 40.5 percent expect the use of subcontractors to grow.

According to the recent ***RAND Corporation*** report, "The Economics of Defense," the cost of managing cyber attacks for contractors will increase by 38 percent, the bulk of which can be attributed to rising costs associated with security programs.

According to the ***Federal Procurement Data System***, the top 100 federal contractors in fiscal year 2014 received a total of $235.93 billion in contract awards. The top 10 recipients of federal dollars raked in $117.7 billion, or about 49.9 percent of all dollars awarded to the top 100 federal contractors.

According to the ***U.S. Small Business Administration (SBA)***, the federal government awarded about a quarter of federal contracts to small businesses in the past year, the highest percentage of contracting dollars awarded to small businesses since a 23 percent benchmark was established by the SBA in 1997.

The White House has requested $178 billion for military hardware in the fiscal year beginning October 1—about $70 billion to develop war-fighting systems, and $108 billion to produce the systems, according to a recent ***Forbes*** article.

▶ Read more

CONTINUED FROM PAGE 1

EXECUTIVE SEMINAR

of bid protests. Contractors must focus on maintaining relationships with key government regulators rather than pursuing aggressive growth strategies at a time when companies are forced to do more with less.

Amid this unpredictable environment, contractors should be deliberate and selective by pursuing fewer, more strategic bids that align with their core capabilities. Firms should be aware that budget constraints could stimulate competition over a smaller pool of resources and procurement needs, so investing heavily in differentiation and innovation around their core capabilities will be instrumental in maintaining a steady stream of business. Though federal defense budgets are shrinking, the energy and technology sectors are undergoing growth and disruption, stimulating a wealth of procurement needs that could prove advantageous to contractors whose capabilities align with material needs in these sectors.

Currently, government procurement is very focused on, and can be partial to, large businesses, which causes a trickle-down effect to smaller businesses and new contractors in the aforementioned growth sectors. However, the industry has historically been cyclical, and that pendulum has and will continue to swing back in favor of small businesses as these sectors evolve and grow.

OPPORTUNITIES ABOUND IN ENERGY AND TECHNOLOGY CORRIDORS, BUT BARRIERS TO INNOVATION EXIST

The industry may see more contractors tapping small businesses in the booming tech and energy sectors. However, a number of barriers to innovation exist in the current business environment, including regulatory and compliance hurdles as well as legal issues. Speakers cautioned that the overall government contracting industry must take steps to ensure that the complex regulatory environment doesn't hamper growth and advancement of R&D in technology and affordable energy.

The Department of Defense (DOD), for example, is looking for opportunities to engage with major technology companies – many based in Silicon Valley – that aren't familiar with the procurement process and may be precluded from entry into the defense space. The heavy regulations and lack of funding make the space risky for these major innovators to contract with the DOD. Furthermore, these companies often receive R&D dollars in much greater sums from other sources, which makes the contracting space less attractive. The DOD will have trouble achieving its goals of technological innovation unless it disrupts its own management and oversight regimes.

DIALOGUE AND EDUCATION INCREASING AMONG CONTRACTORS AND GOVERNMENT AGENCIES

If there's one thing defense contractors can count on, it's that Defense Contract Audit Agency (DCAA) audits will always pose regulatory and compliance challenges. Contractors need to ensure their business systems are regularly monitored for adequacy and compliance, so that when the DCAA issues an audit, companies will have a plan in place to address any gaps. The good news is that there is a renewed emphasis on compliance and the industry is encouraging a two-way feedback system with government oversight bodies – in other words, the government is listening.

Government contractors control their own destiny and should embrace their own affirmative duty to self-report information about any potential violation of a criminal law, including fraud, overpayment, bribery or criminal conflicts of interest. Companies must remember that negative conduct, especially fraud, is first and foremost personal and, therefore, they must establish rigorous employee conduct standards as their first line of defense against fraud and other violations.

Contractors should also educate themselves on the Mandatory Disclosure Regulations embedded within the Federal Acquisition Regulations (FAR), and establish a written code of ethical conduct to establish proper practices of self-policing, including specific accountability standards and procedures for internal audit. Proper training is essential to promoting a culture of compliance, as lack of knowledge or procedure does not absolve companies of risk or potential for punitive measures.

LOOKING AHEAD FOR GOVERNMENT CONTRACTORS

As the speakers discussed, there are macro and micro factors impacting the procurement landscape, with innovation and compliance the top two drivers of growth in this space. Business system audits and proper accounting standards are important for successful partnerships and sustained growth. Government contractors can benefit from upfront preparation, which can reduce risk and save them added effort down the line when engaging openly with the DCAA or DCMA. In an increasingly competitive landscape, contractors can stay ahead by practicing due diligence regarding compliance and legal matters, thereby maximizing their existing position within the industry.

For more information, please contact:

Christopher Carson, National Government Contracting Practice Lead at 703-770-6346 / ccarson@bdo.com

Eric Sobota, Partner In Charge, Government Contracts and Grants Advisory Services at 703-770-6395 / esobota@bdo.com

Robert Craig, Managing Director at 703-770-1095 / rcraig@bdo.com

John Van Meter, Managing Director at 703-893-0600 / jvanmeter@bdo.com

▶ Read more

MANAGING CONTRACTORS' CYBERSECURITY RISKS

By Bob Craig and Karen Schuler

The need for strong security measures to protect sensitive government data from hackers has never been more intense.

In November 2014 alone, the federal government suffered at least four breaches of its information systems, including cyber-attacks on the U.S. Postal Service, the State Department, NOAA and the White House. But more recently – and perhaps more troublingly – the Office of Personnel Management suffered a data breach that compromised the personal information of millions of federal employees and contractors. In fact, analytics firm BitSight Technologies recently found that defense contractors' security systems were **consistently more vulnerable** than those of retailers who have experienced their own cyber breaches, such as Home Depot, Target and eBay. What these news stories don't cover, however, is the fact that much of the burden of securing government data falls on contractors.

Many contractors have begun to take proactive steps to establish internal controls designed to protect sensitive information and respond quickly and effectively to unauthorized intrusions. However, these efforts alone may not be enough to halt the proliferation of cyber attacks on contractors and federal entities. Luckily, the federal government is taking steps to clarify contractors' obligations and requirements for data security, with the goal of creating a standardized approach to preventing and addressing cyber attacks.

BACKGROUND & OVERVIEW

The federal government has struggled to adopt a unified and mandatory approach to contractor data security, with each agency independently adopting cybersecurity requirements. As a result of this ad hoc approach, contractors face a confusing and often conflicting set of requirements from the agencies they support. The Department of Defense (DOD) recently adopted a new set of regulations governing unclassified controlled technical information, which has the potential to set the standard for the rest of the industry. It does this by incorporating the Department of Commerce's National Institute of Standards and Technology (NIST) draft version of Special Publication 800-171 (NIST SP 800-171), Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

The new NIST guidelines are directed at contractors where controlled unclassified information (CUI) is processed, stored or transmitted. The final version of NIST SP 800-171 will attempt to synthesize the federal government's recommendations to contractors for ensuring the confidentiality of sensitive information stored on their systems.

APPLICABILITY

NIST SP 800-171 establishes an open and uniform program for managing sensitive information that requires safeguards or dissemination controls. NIST SP 800-171 is intended for use by federal agencies that provide controlled unclassified information (CUI) to government contractors, or when CUI is developed by those contractors for the government. In other words, this is applicable to agencies sharing data (including CUI) with contractors for purposes such as designing or manufacturing products, or providing services to the U.S. government.

More specifically, NIST SP 800-171 will provide federal agencies with recommended requirements for protecting the confidentiality of CUI when:

1. The CUI is resident in non-federal information systems and organizations;
2. The CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation or government-wide policy for the CUI category or subcategory listed in the Registry; or
3. The information systems where the CUI resides are not operated by organizations on behalf of the federal government.

REQUIREMENTS

Security requirements for protecting the confidentiality of CUI within a contractor's information systems have a well-defined structure consisting of a basic section and a derived section. The basic security requirements are obtained from the Federal Information Processing Standard Publication 200 (FIPS Publication 200), which provides the high-level and fundamental security requirements for federal information and information systems. The derived security

▶ Read more

CONTINUED FROM PAGE 3

CYBERSECURITY RISKS

requirements are taken from the security controls in NIST Special Publication 800-53. Starting with FIPS Publication 200, security requirements and controls are tailored to eliminate provisions that are uniquely federal and not directly related to protecting the confidentiality of CUI or expected to be routinely satisfied by nonfederal organizations without specification.

For ease of use, security requirements are organized into 14 families. Each family contains the requirements related to its general security topic. The families are closely aligned with the minimum security requirements for federal information and information systems described in FIPS Publication 200.

Security Requirement Families
Access Control
Awareness and Training
Audit and Accountability
Configuration Management
Identification and Authentication
Incident Response
Maintenance
Media Protection
Personnel Security
Physical Protection
Risk Assessment
Security Assessment
System and Communications Protection
System and Information Integrity

BEST PRACTICES FOR CONTRACTORS

Although the government has long recognized the need for security measures to protect sensitive government information residing on contractor systems, it has struggled to adopt a unified approach to contractor data security. NIST Special Publication 800-171 aims to rectify this situation and provide clear, government-wide security requirements for CUI, which take into account the unique circumstances for non-federal entities dealing in sensitive data.

That said, there are a number of general best practices all businesses, including contractors, can implement to further help secure their information and maintain compliance:

- **Develop a unified threat management program.** Organizations should assess all of their IT systems and locations of sensitive data, and identify where any vulnerabilities may exist. It may be helpful to establish a risk or governance committee to coordinate and centralize this initiative.

- **Establish and promote a strong internal controls environment.** Contractors should implement policies explicitly outlining access levels for certain information and establish procedures for continuous monitoring, training and documentation, which helps employees stay up-to-date on the latest threats.

- **Develop a threat response plan.** As always, it is best for companies to take a proactive approach to dealing with cyber threats, rather than waiting until a crisis emerges. This includes developing a response team (which may include legal, compliance and IT personnel) to handle threats as they arise, as well as establish protocols for identifying, isolating and eradicating threats. The response plan should also address ways to recover from the breach – bringing IT systems back online, patching vulnerabilities, etc. – and lessons learned to help improve policies and procedures in the future. And, finally, test the plan. Tabletop exercises provide organizations the ability to identify and address gaps in the plan before the time arises to use it.

Preventing and addressing cyber attacks is a moving goalpost for both contractors and the federal government. However, a combination of proactive, enterprise-wide threat reduction and regulatory standard-setting could go a long way toward helping contractors better meet their obligations to the government.

For more information, contact Bob Craig, Managing Director with BDO Government Contracting Advisory Services, at rcraig@bdo.com, or Karen Schuler, Managing Director with BDO Consulting, at kschuler@bdo.com.

BDO WELCOMES NEW PROFESSIONALS TO GOVERNMENT CONTRACTS ADVISORY SERVICES GROUP

BDO's Government Contracts Advisory Services (GCAS) group is pleased to announce that it has added **Thomas Fuchs** and **Dexter Tucker** to its team in McLean, Va. Both Tom and Dexter join the group as Managing Directors, supporting GCAS's national efforts to grow its service offerings and footprint.

Tom Fuchs brings more than two decades of experience in commercial product and services contracting to GCAS. He will be developing the group's Federal Supply Schedule/Commercial Pricing practice, leveraging his extensive experience in General Services Administration and Veterans Affairs Federal Supply Schedule programs, commercial contracting, state and local government contracts and cooperative purchasing organizations.

Dexter Tucker joins GCAS from BDO Consulting, and will lead the Enterprise Software Solutions practice. With more than 25 years of experience in enterprise resource planning (ERP) and enterprise resource management (ERM), Dexter will help expand BDO's ERP and ERM systems service offerings, provide selection and evaluation advisory support to clients, and manage implementation and configuration efforts for client business information systems. Also joining the Enterprise Software Solutions practice will be Senior Manager Ricardo Alvarado.

*"Tom and Dexter are valuable and welcomed additions to the GCAS team," said **Chris Carson, leader of the Government Contracting practice at BDO**. "Their significant experience and specialized knowledge will be instrumental in helping us continue to refine and enhance our service offerings to better support our clients nationwide."*

For more information, please contact Tom Fuchs at tfuchs@bdo.com or Dexter Tucker at dtucker@bdo.com.

▶ Read more

SUPPLY CHAINS – NO STRONGER THAN THEIR WEAKEST LINK

Top Considerations to Take Control of Your Supply Chain

By Bob Craig

Government contractors face ever-growing challenges in managing their suppliers as the government contracting industry and its regulatory environment evolve.

Prime and upper tier contractors are expected to have more insight into and control over their supplying subcontractors' behavior and compliance than ever before. At the same time, regulatory requirements continue to grow more robust and demand more of contractors' time, money and oversight.

Below are several important risk areas for contractors to keep in mind as they consider their supply chains and oversee their subcontractors:

COUNTERFEIT PARTS REGULATIONS

Incidences of counterfeit or suspected counterfeit products have increased in recent years. The National Defense Authorization Act (NDAA) instructs the Department of Defense (DOD) to keep counterfeit items out of its supply chain, and spreads responsibility for doing so along the entire federal procurement chain, leaving contractors and subcontractors open to the risks and liabilities associated with compliance. Inclusion of counterfeit parts in a deliverable under a government contract can be considered a breach of contract, which can trigger a Termination for Default and a False Claims Act investigation. Additionally, the DOD recently adjusted its definitions of counterfeit and suspect-counterfeit parts to include only electronic parts, defining a counterfeit item as "an unlawful or unauthorized reproduction, substitution or alteration that has been knowingly mismarked, misidentified or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer."

To ensure that counterfeit materials, including obsolete electronics, do not present a threat to U.S. personnel and the government's activities, the DOD places the burden on all contractors providing electronic parts to the government to take proactive steps to detect counterfeit components and prevent them from entering the federal supply chain. If a contractor becomes aware of the existence of counterfeit parts in its supply chain, it is obligated under the Mandatory Disclosure rule to notify the Contracting Office of non-compliance. The most recent NDAA has instituted new requirements for the presence of an operational system meeting a strict 12-part criterion to identify and avoid counterfeit parts. In addition, several revisions have been implemented or proposed to strengthen requirements around avoiding counterfeit parts, including DFARS Case 2012-D050: Supply Chain, DFARS Case 2012-D042: Business Systems Compliance , FAR Case 2012-024: Commercial and Government Entity Code , FAR Case 2012-032: Higher-Level Contract Quality Requirements and FAR Case 2013-002: Expanded Reporting of Nonconforming Supplies.

PRIME CONTRACTORS' RESPONSIBILITY FOR PRICE REASONABLENESS OF SUBCONTRACTORS

FAR Subpart 15-4 provides guidance for determining and negotiating a fair and reasonable price for the prime contract and any contract modifications, including subcontractor costs. Though the FAR does not explicitly define what constitutes a "fair and reasonable" price, the provisions clearly outline the need for a contracting officer to determine the fairness of the contractor's pricing before awarding a contract or placing orders.

The FAR mandates that the prime contractor must conduct cost or price analysis to establish price reasonableness, include results of these analyses in the price proposal and submit subcontractor cost and pricing data to the government as part of its own data and proposal in certain circumstances. Any prime or upper tier contractor that is required to submit cost or pricing data is also required to analyze cost data before awarding any subcontracts, purchase orders or contract modifications.

CONFLICT MATERIALS/ MINERALS REGULATION

Electronics companies are required by the SEC, per the Dodd-Frank Wall Street Reform and Consumer Protection Act, to disclose their use of conflict minerals if those materials are necessary to the function or production of a product. Conflict minerals include tungsten, tin, gold and tantalum (3TG), frequently used in consumer electronic devices, among other products, which are often mined in areas controlled by rebel groups committing human rights violations.

Since the rule was instated, companies across the country that manufacture a wide variety of items, including computers, medical implants and more, have scrambled to comply with the act's disclosure mandates. The requirement brings up a variety of costs and liabilities along the supply chain, since tracing small amounts of 3TG back to their source can be difficult. The SEC has implemented a three-step process for complying with the rule, including determining the applicability of the rule, conducting a reasonable country of origin inquiry (RCOI) for any applicable materials and filing a completed and audited Conflict Minerals Report to the Form SD (if required to file).

COMMERCIAL ITEM DETERMINATION (CID)

A key part of the procurement process is determining whether the acquisition of supplies or services meets the government's

▶ Read more

CONTINUED FROM PAGE 5

SUPPLY CHAINS

commercial item designation. The Federal Acquisition Streamlining Act (FASA) of 1994 established that the government must conduct research to determine if its needs can be met by supplies or services that can be defined as commercial items by the FAR. For contractors, FAR 2.101 provides criteria for designating an item or service as "commercial." In recent years, we have seen numerous instances of subcontractor CIDs being overturned, most commonly in instances where contractors were forced to provide evidence of a cost reasonableness analysis of their suppliers where only price analysis had been performed in the past. Conducting cost reasonableness analyses for subcontractors can become extremely difficult if the subcontractor is reticent to open its books and records to another organization.

In 2014, the Department of Defense purchased over $60 billion in commercial Items. In February, the Office of the Under Secretary of Defense issued a memorandum which stated that "the determination of an item described as 'commercial of-a-type' has been difficult for Contracting Officers." In order to assist in the determination of a commercial item, the DOD has recently established a Commercial Item Pricing cell within DCMA's Cost & Pricing Center to focus on this area and is updating its Commercial Item Handbook.

SMALL BUSINESS SUBCONTRACTING REQUIREMENTS

Part of Congress' broad authority to impose requirements on the federal acquisition process includes measures to promote and incentivize federal agencies to award a "fair proportion" of contracts and subcontracts to small businesses. Specifically, FAR 19.702 states that any contractor awarded a contract for an amount greater than the simplified acquisition threshold – generally $150,000 for most contracts – must offer the maximum practicable opportunity to small businesses while still yielding efficient results.

The Small Business Act also imposes a number of requirements on businesses contracting or subcontracting with small businesses that can prove burdensome for some contractors. Section 8(d) requires that large businesses awarded a bid or contract exceeding $750,000 (or $1.5 million for construction efforts) that has "subcontracting possibilities" must submit an acceptable subcontracting plan. The plan should include specific dollar and percent goals for subcontracting to small, small Historically Underutilized Business Zone (HUBZone), small disadvantaged, small women-owned, small veteran-owned and service-disabled veteran-owned small business firms.

CYBERSECURITY ISSUES CREATED BY SUBCONTRACTOR ACCESS TO PRIME CONTRACTORS' SYSTEMS

The federal government has not been immune from the proliferation of cyber threats and attacks in recent months and years. Such breaches raise questions around whether federal agencies or contractors hold responsibility for information security and cybersecurity during the procurement process. Federal contractors working with subcontractors face cyber risks not only from outside sources and hackers, but also from subcontractors who have access to internal systems, data and proprietary information. Suppliers that have access to certain of the prime contractor's systems and equipment could pose a significant threat. It is important that prime contractors properly vet all suppliers to ensure that they are a trusted source, as well as limit supplier access to only the systems or equipment necessary to perform the work.

Prime and subcontractors are subject to stringent protective measures around unclassified controlled technical information (UCTI) residing on their networks. Specifically, the Defense Federal Acquisition Regulation Supplement Final Rule states that government contractors possessing any UCTI must provide adequate security for their technology and networks, as well as promptly report a wide range of cyber incidents to the contracting department. Prime contractors are responsible for ensuring that their subcontractors' unclassified information systems comply with these regulations, as well. Given the wide range of data and technical information covered within these rules, prime contractors face extensive obligation and liability around cybersecurity. (For more information on cybersecurity, please refer to our article on page 3.)

FLOW-DOWN CLAUSES

A contracting agency may require that certain sections of its contract apply to subcontractors, but because subcontractors hold contracts with prime contractors rather than the government, the requirement must be explicitly included in the contract between prime and subcontractor. FAR 9.104-4 states that prospective contractors are required to determine the responsibility of their various subcontractors. A flow-down clause is a common practice for ensuring consistency and that the contractual obligations imposed on prime contractors are upheld by subcontractors, as well.

Common flow-down clauses include product or quality specifications, guidelines for dispute resolution, federal regulatory requirements, scope of work, ethics and mandatory disclosure, certified cost and pricing data, Cost Accounting Standards and small business plans . In many cases, it is not clear to the prime contractor exactly which clauses must be incorporated into the subcontract, so contractors have favored a blanket approach to flow-down clauses, using the entire prime contract for subcontractors with only slight alterations. This often leads to a delayed procurement process and adds confusion to the subcontractor's compliance requirements.

Prime and subcontractor relationships can be complex and varied, but with proper planning and awareness of relevant compliance standards, you can secure your supply chain and ensure that the subcontracting process runs more smoothly.

For more information, please contact Bob Craig, Managing Director with BDO Government Contracting Advisory Services, at rcraig@bdo.com.

▶ Read more

SIGNIFICANT ACCOUNTING & REPORTING UPDATES

Revenue Recognition Updates

FASB Issues Proposal to Defer Revenue Standard by One Year

On July 9, the Financial Accounting Standards Board (FASB) FASB decided to delay the effective date of the new revenue standard (ASU 2014-09, Revenue from Contracts with Customers) by one year.. For public entities that follow U.S. GAAP, the deferral results in the new revenue standard being effective for fiscal years, and interim periods within those fiscal years, beginning after December 15, 2017. Nonpublic entities are required to apply the new revenue standard for fiscal years beginning after December 15, 2018, and interim periods within fiscal years beginning after December 15, 2019. The FASB decided, that a deferral is necessary to provide adequate time to effectively implement the new revenue standard.

Aerospace and Defense Revenue Recognition Task Force

The AICPA's Aerospace and Defense Revenue Recognition Task Force (A&D Task Force) has been working to identify implementation issues and develop a new Accounting Guide on Revenue Recognition. The following are the current implementation issues identified by the A&D Task Force that have been submitted to the AICPA's Revenue Recognition Working Group and Financial Reporting Executive Committee:

- Acceptable measures of progress for performance obligations satisfied over time in A&D contracts, and how to account for incremental costs to fulfill a contract (including uninstalled materials and wasted materials);
- Treatment of contract costs for the various measures of progress (including pre-contract costs);
- Constraint of revenue impact of variable pricing (incentive fees, award fees, economic price adjustments, etc.) and impact of subsequent events;
- Accounting for contract modification, unpriced change orders, claims and considerations needed to assess whether a significant component exists in determining the transaction price for various types of contracts; and
- Significant financing component.

To date, the A&D Task Force has not finalized guidance on the identified implementation issues; however, government contractors should be monitoring these developments as part of their implementation efforts. See the AICPA's website for further status of implementation issues.

FASB and IASB Agree to Clarify Principal versus Agent Guidance

Reselling to the federal government can be a significant part of a company's business and a meeting of the FASB and IASB on June 22, 2015, could impact the way federal contractors recognize revenue (gross versus net revenue reporting) based on the new control principle and additional clarifications.

At their meeting, the FASB and IASB discussed potential amendments to the new revenue standard's guidance on assessing whether an entity is a principal or an agent. They also tentatively agreed on amendments to clarify the application of the overall principle, amend the indicators to better align with the principle, and revise and add examples. While the proposed amendments will provide clarity to government contractors, the complex nature of many prime or subcontract arrangements will not eliminate the judgments related to principal versus agent assessments. See the FASB's website for further information.

PCAOB Auditing Standard - (AS) No.18, Related Parties

In 2014, the Public Accounting Oversight Board (PCAOB) adopted several standards and amendments, including Auditing Standard (AS) No. 18, Related Parties, and amendments to certain PCAOB auditing standards regarding significant unusual transactions, among others. AS No. 18 supersedes the PCAOB's interim auditing standard, AU sec. 334, Related Parties. This auditing standard will require a company's public accounting firm to strengthen its procedures in those areas that have been associated with risks of incorrect or fraudulent financial reporting. This auditing standard will heighten focus on the organization's named executive officers, as well as other influential senior executives or management.

As a result of AS No. 18, government auditors, such as Defense Contract Audit Agency (DCAA), require audit risk assessments to include details on the effect of related-party transactions. Additionally, DCAA will likely incorporate any findings of deficiencies noted by a company's public accounting firm in its audit procedures.

Companies without adequate policies and procedures to address this auditing requirement should consider adopting written documentation addressing the collection and management of financial transactions (e.g., employment contracts, severance agreements, incentive plan documents, award agreements, post-employments, arrangements, etc.).

This standard will be in effect for fiscal years beginning on or after Dec. 31, 2014, including reviews of interim financial information within these fiscal years.

FASB Issues Guidance for Accounting for Fees Paid in a Cloud Computing Arrangement

The FASB has issued an ASU to clarify that if a cloud computing arrangement contains a software license, a customer should account for this element consistent with the acquisition of other software licenses that are capitalized. Otherwise, a customer should account for the arrangement as a service contract, which would usually be expensed. The new standard takes effect in 2016 for public companies.

FASB Implements Practical Expedient for Measuring Defined Benefit Plan Obligations and Assets

The FASB recently issued an update providing companies an optional practical expedient for measuring an employer's defined benefit obligation and plan assets when the company's fiscal year-end does not fall on the

▶ Read more

CONTINUED FROM PAGE 7

ACCOUNTING & REPORTING UPDATES

last day of the month. In this situation, an entity may elect to measure defined benefit plan assets and obligations using the month-end that falls closest to its fiscal year-end. The new standard takes effect in 2016 for public companies.

FASB Issues ASU to Simplify Presentation of Debt Issuance Costs

The FASB has issued an update intended to simplify U.S. GAAP by changing the presentation of debt issuance costs. Under the new standard, debt issuance costs will be presented as a reduction of the carrying amount of the related liability, rather than as an asset, consistent with debt discounts. The update takes effect retroactively in 2016.

FASB Issues ASU to Simplify Consolidation Analysis

The FASB recently changed its consolidation guidance, which could significantly impact certain entities. The new ASU simplifies U.S. GAAP by eliminating entity-specific consolidation guidance for limited partnerships. It also revises other aspects of the consolidation analysis, including assessments of kick-out rights, fee arrangements and related parties. The amendments rescind the indefinite deferral of FASB Statement No. 167 for certain investment funds, replacing it with a permanent scope exception for money market funds. The new standard takes effect in 2016 for public companies.

FASB Eliminates Concept of Extraordinary Items from U.S. GAAP

The FASB recently published an ASU to eliminate the concept of extraordinary items from U.S. GAAP. However, the presentation and disclosure guidance for items that are unusual in nature *or* occur infrequently will be retained and expanded to include items that are both unusual in nature *and* infrequently occurring. The new standard takes effect in 2016.

FASB Issues Accounting Alternative for Private Companies on Intangible Assets in Business Combinations

The FASB recently issued new guidance intended to improve financial reporting for private companies establishing an accounting alternative for certain intangible assets acquired in a business combination. If a private company elects the alternative method, it would not separately recognize from goodwill and certain assets arising from customer relationships and or noncompetition agreements upon acquisition. Rather, they would be subsumed into goodwill, and the goodwill would be amortized. The alternative is intended to reduce cost and complexity for private companies. The decision to elect the alternative must be made at the time upon the occurrence of the first in-scope transaction in fiscal years beginning after Dec. 15, 2015, with early application permitted.

FASB Issues Proposal to Reduce Complexity in Stock Compensation Accounting

On June 8, 2015, the FASB issued a proposed Accounting Standards Update (ASU), *Improvements to Employee Share-Based Payment Accounting*, to amend ASC Topic 718, *Compensation – Stock Compensation.* Comments to the proposed update are due Aug. 14, 2015. The proposal aims to identify, evaluate and improve areas of GAAP while maintaining or improving the usefulness of information in financial statements. The proposed simplifications address a variety of aspects of the accounting process for share-based payment transactions. The proposal includes certain provisions specific to non-public companies, including use of a practical expedient for determining the expected term, and providing a one-time opportunity for a non-public company to change its measurement basis to intrinsic value for all liability-classified awards. The proposals could significantly change net income and have far-reaching impact for government contractors.

See the FASB's website for further information.

SEC Proposes Pay vs. Performance Disclosures

On April 29, 2015, the Securities and Exchange Commission proposed rules implementing requirements mandated by Section 953(a) of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The proposed rules would require registrants to clearly disclose the relationship between executive compensation actually paid and the financial performance of the registrant. The proposed rules are intended to help better inform shareholders when they vote to elect directors or conduct advisory votes on executive compensation.

SEC Adopts Amendments to Regulation A

On March 25, 2015, the Securities and Exchange Commission unanimously approved amendments to Regulation A. The amendments, known as "Regulation A+," were required by Section 401 of the JOBS Act. They are intended to increase smaller companies' access to capital by modernizing Regulation A and expanding it to provide a streamlined process by which a private company can offer and sell up to $50 million of securities in a 12-month period. The adopting release, No. 33-9741, is available here.

Further BDO highlights on accounting and reporting updates can be found here.

▶ Read more

REGULATORY UPDATES

Final DFARS Rules

Case 2014–D009: Effective May 26, 2015, the Department of Defense (DOD) issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to clarify that entering into a contract award may cause a small business to eventually exceed the applicable small business size standard.

Case 2014-D020: Effective May 26, 2015, DOD issued a final rule amending DFARS to establish the approval authority for time-and-material and labor–hour contracts and task orders with determinations and findings above the $1 million threshold; these contracts now must be approved one level above the contracting officer. The approval requirements in this rule do not apply to contracts that support contingency or peacekeeping operations, or provide humanitarian assistance, disaster relief, or recovery from conventional, nuclear, biological, chemical or radiological attack.

Case 2014-D015: Effective May 26, 2015, DOD issued a final rule requiring contracting officers to consider information in the Statistical Reporting module of the Past Performance Information Retrieval System when evaluating contractors' past performance under competitive solicitations for supplies using simplified acquisition procedures, including those valued at less than or equal to $1 million under FAR 13.5.

Interim DFARS Rules

Case 2015-D028: DOD issued an interim rule to amend the DFARS to clarify the requirements associated to indirect offset costs incurred under Foreign Military Sales (FMS) agreements. A revision has been made to DFARS 255.7303-2, "Cost of doing business with a foreign government or an international organization," by adding paragraph (a)(3)(iii) to provide guidelines for contracting officers to implement when an offset in indirect costs is a condition of the agreement.

Proposed FAR Rules

Case 2014-003: DOD, GSA and NASA proposed to amend the FAR to implement changes made by the Small Business Administration's (SBA) final rule (78 FR 42391) issued July 16, 2013, concerning small business contracting. SBA's final rule and FAR's proposed rule implement statutory requirements set forth in sections 1321 and 1322 of the Small Business Jobs Act of 2010 (Jobs Act – Pub. L. 111-240). Section 1321 requires subcontracting compliance related to small business concerns, contracting, program and small business offices, and periodic review and oversight of activities performed. Section 1322 of the Jobs Act amended the Small Business Act (15 U.S.C. 367 (d)(6)) to include the requirement of prime contractors to use a small business subcontractor to the extent that the prime contractor relied on and used the small business in preparing and submitting its bid or proposal to win an award. In the event that a prime does not utilize a small business subcontractor as described in the bid/proposal, the prime contractor is required to provide a written explanation to the contracting officer why it is unable to do so. This proposed FAR rule implements the requirement for funding agencies to receive a small business subcontracting credit for all contract vehicles. Prime contractors also will have to submit a Summary Subcontract Report (SSR) for DOD and NASA contracts annually, rather than semi-annually, and the rule deletes the requirement for the prime contractor to submit a separate report to each DOD component for construction, related maintenance and repair contracts.

Case 2014-025: The FAR Council and Department of Labor (DOL) published their proposed regulations and guidance for implementing President Obama's Fair Pay and Safe Workplaces executive order requiring contractors to disclose certain labor violations to the government. The phased approach consists of focusing on the 14 federal labor laws and postpones state labor laws for a later date.

The Executive Order (E.O.) creates new responsibilities for agencies to require established practices to assist contractor (and subcontractors) in complying with labor laws and to designate an Agency Labor Compliance Advisor (ALCA) to assist in evaluating contractor disclosure. Contractors will have to report labor violations when applying for contracts and on a semiannual basis. DOL's Guidance offers details on various key terms used throughout the E.O., how agencies should determine what is a reportable violation, what information to disclose regarding a violation, how to analyze the severity of labor violations, and the role of the ALCA, DOL and other enforcement agencies in addressing violations.

Under the proposal, contractors are required to collect information on labor violations from their subcontractors and determine whether the subcontractor is a responsible source. The proposed rule would allow prime contractors to seek the DOL's assistance in evaluating subcontractor labor violations and making determinations of responsibility. One potential approach, which is also seeking comments, is to require subcontractors to report violations directly to DOL, rather than the prime contractor.

Case 2014-018: DOD, GSA and NASA are proposing to amend the FAR to remove the distinction between DOD and non-DOD agency areas of operation applicable for the use of FAR clause 52.225–26, "Contractors Performing Private Security Functions Outside the United States." As a result, all policies regarding defense contractors performing private security functions would be contained in the DFARS. This rule also proposes to add a definition of "full cooperation" to FAR 52.225-26 in order to affirm that the contract clause does not foreclose any contract rights arising in law, the FAR or the term of the contract when cooperating with any government-authorized investigation into incidents reported pursuant to the clause.

Final FAR Rule

Case 2014–022: On July 2, 2015, a final rule issued under the joint authority of DOD, GSA and NASA amends the FAR to implement 41 U.S.C. 1908, which requires an adjustment every five years of acquisition-related thresholds for inflation using the Consumer Price Index. Below are the Inflation Adjustment of Acquisition-Related Thresholds:

- The micro-purchase base threshold of $3,000 (FAR 2.101) is increased to $3,500.
- The simplified acquisition threshold (FAR 2.101) of $150,000 is unchanged.

▶ Read more

CONTINUED FROM PAGE 9

REGULATORY UPDATES

- The FedBizOpps pre-award and post-award notices (FAR part 5) remain at $25,000 because of trade agreements.
- The threshold for use of simplified acquisition procedures for acquisition of commercial items (FAR 13.500) is raised from $6.5 million to $7 million.
- The cost or pricing data threshold (FAR 15.403–4) and the statutorily equivalent Cost Accounting Standard threshold are raised from $700,000 to $750,000.
- The prime contractor subcontracting plan (FAR 19.702) floor is raised from $650,000 to $700,000, and the construction threshold of $1.5 million remains the same.
- The threshold for reporting first-tier subcontract information including executive compensation will increase from $25,000 to $30,000 (FAR subpart 4.14 and 52.204–10).

Case 2013-012: Effective June 8, 2015, a final rule has been issued to amend the FAR, implementing section 802 of the NDAA for FY 2013. This section provides additional requirements relative to the review and justification of pass-through contracts. Pursuant to FAR 52.215-22, in instances where an offeror informs the agency of its intentions to award more than 70 percent of the total cost of work to be performed under the contract, task order or delivery order to a subcontractor, section 802 requires the contracting officer to:

1. Consider the availability of alternative contract vehicles and the feasibility of contracting directly with a subcontractor(s) that will perform the majority of the work;
2. Make a written determination that the contracting approach selected is in the government's best interest; and
3. Document the basis of such determination.

These requirements are being implemented in FAR 15.404-1(h) for consistency purposes, and are applicable to all agencies subject to FAR even though section 802 applies to DOD, the State Department and USAID only. Revisions to FAR 15.404-1(h)(2) clarify that competition requirements still apply if the contracting officer selects alternate approaches. Revisions to FAR 15.404-1(h)(3) clarify that the requirements of this rule do not apply to small business set-aside contracts.

Other

Department of State Final Rule: Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards: The Department of State finalized its portion of the uniform federal assistance rule issued by OMB. The Department adopted part 200 and the agency-specific addendum in the new part 600. These changes have been implemented in the interim final rule and adopted with no modifications. The Department also removed 22 CFR parts 135 and 145, as they were superseded by the publication of the interim final rule.

GSA's New Website to Search for Hourly Labor Rates: The Contract Awarded Labor Category (CALC) website is now live and ready for government acquisition corporations and contractors. This tool provides a convenient way to conduct market research on professional service labor categories and take the guesswork out of cost estimations. Current year rates are provided, and users have the option of searching by specific GSA contract. Results shown are actual awarded hourly rates from GSA services schedules, which allows contractors to search their competition and the government to make informed decisions. The CALC website is available at CALC.gsa.gov.

Revised Non-Foreign Overseas Per Diem Rates: DOD issued a notice on May 28, 2015, that the Defense Travel Management Office is publishing Civilian Personnel Per Diem Bulletin Number 296 in the Federal Register. This bulletin lists revised per diem rates for U.S. Government employees for official travel in Alaska, Puerto Rico the Northern Mariana Islands and Possessions of the United States, when applicable, to assure travelers are paid the most recent per diem rates.

Federal Acquisition Circular 2005-82: *Small Entity Compliance Guide*: Under the joint authority of DOD, GSA and NASA, the Small Entity Compliance Guide was prepared under section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996. Consisting of a summary of rules appearing in the Federal Acquisition Circular (FAC) 2005-82, it amends the FAR's Equal Employment and Affirmative Action for Veterans and Individuals with Disabilities rule (FAR Case No. 2014-013). Further information about the rules can be found at FAC 2005-825 or http://www.regulations.gov.

DCAA FY 2014 Report to Congress: On March 25, 2015, the Defense Contract Audit Agency (DCAA) released its Report to Congress for FY 2014 Activities. As of Sept. 30, 2014, the agency's workforce consisted of 5,131 employees. 4,556 (or 88 percent) of its staff are auditors with a bachelor's degree, 37 percent have a higher level degree, 25 percent are Certified Public Accountants, and 5 percent have other professional certifications.

During FY 2014, DCAA examined $182.6 billion in contract costs, issued 5,688 audit reports, and identified $4.5 billion in net savings to the government, the warfighter and taxpayers. This produced a return on investment of almost $6.90 for every $1. Despite the increase of examined contract costs, the amount of recommended reductions in proposed or claimed contractor cost decreased 3.9 percent from FY 2013 to 5.9 percent in FY 2014. The lower amount of forward pricing rate activity, which is the area with the highest level of questioned costs, is the cause of the reduction. Forward pricing dollars examined decreased $38.2 billion (or 38 percent), and questioned costs related to forward pricing work decreased $4.6 billion (39 percent) compared to the prior fiscal year.

Additionally, the number of audits performed in FY 2014 took a dive in comparison to FY 2013. Below is a table summarizing the number of audit reports issued:

Type of Audit Report	Number of Audit Reports	
	2014	2013
Forward Pricing	1,089	1,316
Special Audits	1,627	1,898
Incurred Cost	1,919	1,899
Other Audits	1,053	1,146
Total	**5,688**	**6,259**

Incurred cost audits have been a major focus of the agency's and its observers. The agency completed 11,101 incurred cost audits during FY 2014, the highest ever since the implementation of its incurred cost teams in 2012. At the end of FY 2014, DCAA had 11,324 adequate annual contractor submissions on hand that were valued at $419 billion. It is

▶ Read more

CONTINUED FROM PAGE 10

REGULATORY UPDATES

awaiting receipt of, or had not yet made an adequacy determination for, an additional 6,861 incurred cost submissions valued at about at $403 billion. Despite these figures, the total year-end balance of 18,185 submissions was 4,924 less than the prior year-end balance of 23,109 (or a 21 percent reduction).

DCAA utilizes a risk-based planning process to help ensure that audit resources focus on the highest-payback areas. Instead of planning audits and making the determination of what to audit based solely on the type of audit being conducted, DCAA examines the risk factors involved, regardless of the audit type. Overseas Contingency Operations (OCO) and Forward Pricing audits were the highest priority during FY 2014. Under the circumstances, both were time sensitive, carried significant risk factors, and would have significantly impacted the government and/or the contracting process had they been deferred. DCAA audited approximately $11.5 billion for OCO contracts and recommended $483 million in reductions.

Access to contractor records continues to be a challenge for the agency. The FY 2013 NDAA, Section 832, mandated documentation requirements for DCAA to gain access to defense contractor internal audit reports. Subsequently, DCAA disseminated the NDAA documentation requirements through formal training, written guidance and inclusion in its CAM. In 2014, the Comptroller General reviewed the documentation DCAA is required to maintain and issued a report to the Congressional defense committee. The report stated that DCAA revised its policies and guidance to incorporate the documentation requirements for requests of companies' internal audit reports as mandated by the NDAA, but noted improvement is needed through the use of examples and definitions, as well as establishing and monitoring internal controls relative to the process.

Additionally, DCAA continues to struggle with contractors allowing access to employees for interviews and observations. Contractors argue that DCAA's access to records does not extend to its employees per FAR 52.215-2(d). FAR 52.215-2(d) specifically gives GAO rights to interview any officer or employee; however, FAR does not specifically support DCAA's efforts to do the same. DCAA submitted a legislative proposal for FYs 2015 & 2016 to support its right to access contractor employees, which would avoid any future confusion and ensure access to employees. This would allow the agency to conduct audits in accordance with GAGAS. The proposal, however, was not incorporated in the FY 2015 NDAA because the House Armed Services Committee's Joint Explanatory Statement (JES) stated that the agency already has the authority to interview contractor employees if such an interview is required to complete the audit. Therefore, DCAA withdrew the legislative proposal from the FY 2016 consideration cycle. DCAA will continue to monitor denials of access to employees and resubmit the legislative proposal if warranted.

PErspective in GOVERNMENT CONTRACTING

Defense firms are targeting commercial cybersecurity companies for acquisition. Massive data breaches are on the rise, affecting both industry and governmental institutions. Businesses and the federal government alike have fallen victim to major cyber attacks perpetrated by state-sponsored hackers in recent months. The June 2015 reveal of a massive breach of the Office of Personnel Management's database, affecting both government workers and contractors, is perhaps one of the most significant attacks seen to date. Amid these threats, the cybersecurity market is very hot – in fact, the industry is expected to grow from $71 billion in 2104 to more than $155 billion by 2019, according to *Homeland Security Today*. Cyber attacks pose a real and growing threat to national security, and defense contractors are looking to boost their offerings in the space, rather than lose out to commercial competitors.

Defense contractor Raytheon recently acquired WebSense for $1.57 billion as part of a wider strategy to tap into the commercial cybersecurity market. *Defense News* reports that the firm has made 14 cyber-related acquisitions since 2007. PE firm Vista Equity Partners financed the WebSense deal, putting up $335 million and retaining a 19.7 percent stake in the firm.

More and more, private equity will be a factor in such defense mergers. With hacks taking place on a daily basis, cutting-edge cybersecurity companies are very much in demand, making it a seller's market. As firms fork out double-digit multiples for the right deal, buyers might need the kind of leverage a PE backer can bring. And with billions of dollars in dry powder, PE firms are in a position to quickly respond to opportunities, according to *Defense News*.

PE firms are also looking to acquire cybersecurity companies as platforms, although high valuations might be prohibitive to some. Bain Capital acquired online security and WAN optimization solutions provider Blue Coat Systems from PE firm Thoma Bravo for $2.4 billion in May. Thoma Bravo previously acquired the company for $1.26 billion in 2012.

Cybersecurity startups are garnering lots of interest from VC firms. According to VC research firm CB Insights, VC firms have invested $7.3 billion into 1,208 cybersecurity startups in the last five years, with the pace and value of deals trending upwards. In 2014, funding exceeded $2 billion for the first time, for a total of 269 deals. Successful startups with stellar offerings will find eager buyers as they eventually enter the M&A pipeline.

As the cybersecurity sector grows and evolves in coming months and cyber companies look for backing, cash-heavy PE firms will likely see a wealth of opportunity for lucrative and innovative deal-making.

PErspective in Government Contracting is a feature examining the role of private equity in the government contracting industry.

▶ Read more

MARK YOUR CALENDAR…

AUGUST 2015

Aug. 17-21
Federal Publications Seminar: Focused Government Contract Costs and Accounting Training
Executive Conference & Training Center
Sterling, Va.

Aug. 25-26
NDIA Navy Gold Coast Small Business Procurement Event*
San Diego Convention Center
San Diego

SEPTEMBER 2015

Sept. 9-11
AIDF Global Disaster Relief Summit*
Ronald Reagan Building & International Trade Center
Washington, D.C.

Sept. 10
GovConnects Cyber 6.0 Conference*
Johns Hopkins University
Kossiakoff Center
Laurel, Md.

Sept. 15-16
Federal Publications Seminar: Contractors' Purchasing Systems Review*
DoubleTree by Hilton
San Diego

Sept. 30
Subcontract Statement of Work Development Best Practices Workshop
Nash & Cibinic Center for Excellence in Government Contracting
Washington, D.C.

OCTOBER 2015

Oct. 4-6
Professional Services Council Annual Conference*
The Greenbriar
White Sulphur Springs, W. Va.

October 15-16
Government Contractor Training Institute*
The Westin San Diego Gaslamp Quarter
San Diego

Oct. 26-27
Navy Small Business Contracting Summit
One Ocean Resort
Jacksonville, Fla.

Oct. 26-30
International Contracting Week
Waterview Conference Center at CEB
Arlington, Va.

* indicates that BDO is attending or hosting this event

CONTACT:

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

ERIC SOBOTA
Partner In Charge, 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

JOHN VAN METER
Managing Director, Government Contracting Advisory Services
703-893-0600 / jvanmeter@bdo.com

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