COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

June 23, 2014

THE GOVERNMENT CONTRACTS UPDATE

FAR COUNCIL PROPOSES EXPANDED REPORTING OF COUNTERFEIT PARTS (79 FED. REG. 33164)

In recognition of the fact that "the problem of counterfeit and nonconforming parts extends far beyond electronic parts and can impact the mission of all Government agencies," the Federal Acquisition Regulatory Council has issued a proposed rule which would revise the Federal Acquisition Regulation ("FAR") to expand reporting requirements for counterfeit and nonconforming items to all contractors doing business with the Federal Government. The rule represents an expansion upon a final rule of the Department of Defense ("DoD") that we reported on here, that required DoD contractors subject to the Cost Accounting Standards to establish a counterfeit part detection and avoidance system for electronic parts. The new proposed rule would require all contractors—not just DoD contractors dealing with electronics products—to report to the contracting officer within thirty (30) days of becoming aware that any "end item, component, subassembly, part or material contained in supplies purchased by the Contractor for delivery to, or for the Government is counterfeit or suspect counterfeit."

In addition, within sixty (60) days of becoming aware that a part is counterfeit or suspect counterfeit or that the item contains a major or critical non-conformance, contractors must report this to the Government-Industry Data Exchange Program ("GIDEP"). A major or critical nonconforming item is a common item that constitutes a "quality escape" (*i.e*, the failure of the supplier's internal quality control system to identify and contain a nonconforming condition) that has resulted in the release of like non-conforming items to more than one customer. In addition, contractors would be required to screen GIDEP reports to avoid the use and delivery of items that are counterfeit or suspected counterfeit items or contain major or critical nonconformance. The proposed rule, however, provides no meaningful guidance on how to comply with the detection and reporting requirements it proposes.

This requirement was implemented in response to Section 818 of the National Defense Authorization Act for FY 2012 (Pub. L. 112-81) ("Act") and Office of Federal Procurement Policy (OFPP) Policy Letter 91-3. Although Section 818 applied only to DoD, the FAR Council concluded that the principles expressed in Section 818 should extend beyond DoD and beyond electronic parts. Similarly, although Policy Letter 91-3 only requires agencies to report to GIDEP, the FAR Council determined that "reporting would be more timely and effective if contractors were to make the reports directly to GIDEP." The Act also provided that a contractor or subcontractor providing a written report as required under the Act would not be subject to civil liability on the basis of such reporting, "provided that the contractor or subcontractor made a reasonable effort to determine that the end item, component, part, or material concerned contained counterfeit electronic parts or suspect counterfeit electronic parts." The proposed FAR clause 52.246-XX(d) includes similar language, but only "if this is a contract with the Department of Defense."

The proposed rule is expected to have a broad impact on contractors of all sizes, because it applies to purchases of commercial items including off-the-shelf items, as well as purchases below the simplified acquisition threshold. Written comments on the rule are due August 11, 2014.

DOD PROPOSES DFARS CHANGE TO REQUIRE ANNUAL REPORTING OF SERVICE CONTRACT DATA (79 FED. REG. 32522)

On June 5, 2014, the DoD issued a proposed rule to revise the Defense Federal Acquisition Regulation Supplement ("DFARS") regarding contractor reporting requirements of service contract data. The proposed rule would require contractors and subcontractors to report annually—at either the end of the fiscal year or the end of contract performance—service contract direct labor hours and corresponding dollar value data in the Enterprise-wide Contractor Manpower Reporting Application ("ECMRA") database. The proposed rule implements section 807 of National Defense Authorization Act ("NDAA") for Fiscal Year 2008, which requires the Secretary of Defense to submit to Congress, no later than June 30th of each year, an annual inventory of service contracts performed during the preceding fiscal year. The data will support DoD in its total force management efforts and in making strategic workforce planning decisions.

Subject to certain exceptions, the reporting requirements would apply to all solicitations, contracts, and task and delivery orders, including FAR part 12 commercial-item acquisitions for (1) services with a total estimated value exceeding the simplified acquisition threshold, or (2) supplies that contain separate line items for services with a total estimated value exceeding that threshold. The new reporting requirements also would apply to all classes of small business concerns and contractors will be required to include the substance of the requirements in subcontracts that "may include services."

Comments on the proposed rule must be submitted by August 4, 2014. DoD has specifically invited comments on the accuracy of the estimated public burden of the new reporting requirements (1.4 hours per response), ways to minimize the burden on the respondents, and ways to enhance the quality, utility, and clarity of the information to be collected.

NIST ISSUES SUPPLEMENTAL GUIDANCE ON ONGOING INFORMATION SECURITY AUTHORIZATIONS

On June 4, the National Institute of Standards and Technology ("NIST") issued a new supplemental guidance document to help agencies move from a static, triennial system of reauthorization of a system's cybersecurity posture to a system of ongoing authorization in connection with Step 5 of NIST's Risk Management Framework. This change comes as a result of a November 2013 Office of Management and Budget ("OMB") memorandum that ordered federal agencies to conduct ongoing authorizations of their information systems and environments in which those systems operate through the implementation of their risk management programs. The November 2013 OMB memorandum also directed NIST to publish guidance establishing a process and criteria for federal agencies to conduct these ongoing assessments and authorizations.

Among other things, NIST's new guidance outlines a transition plan from a static system of authorizations to ongoing authorization and the system and organizational conditions for implementation. In particular, the guidance provides that information systems being transitioned must (1) have been granted an initial authorization to operate by an authorizing official as a result of a "complete, zero-base review" of the system and have entered into operations/maintenance phase of the system development lifecycle; and (2) have an organizational Information Security Continuous Monitoring ("ISCM") program in place that monitors all implemented security controls with the

appropriate degree of rigor and at frequencies specified by the organization in accordance with the ISCM strategy and NIST guidance.

This is the first of three major updates to NIST guidance supporting the Risk Management Framework and the transition to ongoing authorization. The second publication, an updated version of its Special Publication 800-37 (instructing agencies how to apply the NIST risk management framework to IT systems) is expected to be released in June.

U.K. GOVERNMENT LAUNCHES CYBERSECURITY "SCHEME"

On June 5, the U.K. Department of Business, Innovation & Skills announced the official launch of the U.K. government's "cybersecurity scheme." Beginning on October 1, 2014, all suppliers bidding for certain personal and sensitive information-handling contracts for the U.K. will have to be certified under the scheme. The scheme's goal is to assist U.K. organizations in defending against common types of cyber attacks, such as phishing and hacking. The U.K. has also released guidance to help organizations to assess their controls before seeking formal certification under the scheme.

FAR COUNCIL ISSUES FINAL RULE EXPANDING EXECUTIVE COMPENSATION CAP (79 FED. REG. 31195)

On May 30, 2014, the FAR council issued a final rule extending a cap on executive compensation (currently $763,029) imposed by section 803 of the National Defense Authorization Act for Fiscal Year 2012 to all contractor employees (versus just senior executives) working on contracts for DoD, National Aeronautics and Space Administration, and Coast Guard. The cap limits the amount contractors can be reimbursed for contractor employee compensation costs incurred after January 1, 2012. Interestingly, the final rule, which replaces without change an interim final rule published June 26, 2013, applies only to contracts entered into on or after the date of the enactment of the 2012 NDAA (December 31, 2011). In contrast, NDAA section 803(c)(2) states that the expanded reach of the compensation cap applies to costs incurred after January 1, 2012 under contracts entered into before, on, or after December 31, 2011. The retroactive application of the NDAA provision is addressed in a separate proposed rule issued on June 23, 2013.

CASE DIGEST

DOJ Urges Supreme Court to Deny Cert in FCA Statute of Limitations Case (*Kellogg Brown & Root Services Inc. et al. v. U.S. ex rel. Carter*, No. 12-1497 (May 27, 2014))

On May 27, the U.S. Department of Justice ("DOJ") filed an amicus brief in the case of *Kellogg Brown & Root Services Inc. ("KBR") et al. v. U.S. ex rel. Carter,* opposing the Supreme Court's review of a ruling by the U.S. Court of Appeals for the Fourth Circuit on the application of the Wartime Suspension of Limitations Act ("WSLA"), 18 U.S.C. § 3287, to the False Claims Act's ("FCA") statute of limitations provision and the Fourth Circuit's interpretation of the FCA's "first-to-file" provision, 31 U.S.C. § 3730(b)(5). The WLSA suspends the statute of limitations for any "offense" involving fraud or attempted fraud until five (5) years after the termination of hostilities. The Fourth Circuit held that the WLSA applies to FCA *qui tam* suits (in addition to suits initiated by the Government) because a civil FCA violation is an "offense" involving fraud against the United States, and that the applicability of the WSLA does not depend on whether the suit was brought by the government or a private relator. In seeking review by the Court, KBR has argued that the WSLA extends the FCA statute of limitations for the government, but not for private relators, and that the law applies to criminal offenses, but not civil offenses.

The FCA generally requires that a suit be brought within six years of the date of the violation, or within three years of the date material facts that provide the basis for the suit were known or should have been known to the responsible government official (so long as the suit is brought within 10 years of the violation). 31 U.S.C. § 3731(b). However, because the WSLA was amended in 2008 to provide for the suspension of limitations not only when the U.S. is "at war," but also when Congress has enacted a specific authorization for the use of the Armed Forces, the interpretation of the applicability of the WSLA by the Fourth Circuit and DOJ could, in theory, eliminate virtually all time limits for the filing of civil and criminal FCA cases against government contractors.

DOJ also agreed with the Fourth Circuit's ruling on the FCA's "first-to-file" provision. That provision bars private relators from filing an FCA suit based on the same facts underlying a pending action. The Fourth Circuit held that the provision applies only when a related suit is "pending" at the time the relator files an action, and therefore does not bar the filing of a new *qui tam* suit when *qui tam* actions raising similar allegations have been dismissed on non-merits grounds. The Fourth Circuit's application significantly limits the "first-to-file" restrictions, and could further open the door for *qui tam* suits under the FCA.

Federal Circuit Sides With VA in Dispute Over Veteran-owned Business Set Asides (*Kingdomware Techs. Inc. v. United States*, Fed. Cir. No. 2013-5042 (June 3, 2014))

On June 3, 2014, the Federal Circuit affirmed the Court of Federal Claim's ruling that the Department of Veterans Affairs ("VA") was not required to set aside a contract for service-disabled veteran-owned small businesses ("SDVOSB") or veteran-owned small businesses ("VOSB") before deciding to use the Federal Supply Schedule ("FSS") for acquisition purposes. At issue was section 8127 of the VA Act of 2006 ("VA Act"), which requires for the purposes of meeting VOSB contracting goals, VA contracting officers to compete contracts if there is a reasonable expectation that two or more VOSB can submit offers at fair and reasonable prices (the "Rule of Two"). Applying the *Chevron* deference standard to what it deemed an ambiguous provision, the majority in *Kingdomware Technologies Inc. v. United States* found that the VA's determination that certain FSS acquisitions fell outside section 8127(d) of the VA Act was not arbitrary, capricious, an abuse of discretion, nor otherwise not in accordance with the law.

Noting the deference afforded to agencies in interpreting statutes that they are assigned to implement, and the "bedrock principle of statutory interpretation that each word in a statute should be given effect," the majority found that it was reasonable for the VA to conclude that the language "for purposes of meeting the [VOSB] goals" meant that the Rule of Two did not have to be applied to every procurement after the agency had met its VOSB contracting goals. Kingdomware argued that section 8127(d) required the VA to award contracts using the Rule of Two because the that section's use of the words "shall award contracts" was an "unambiguous imperative that the Secretary can never use the FSS where the Rule of Two may be satisfied." However, the majority agreed with the VA's argument that such an interpretation would read out the statute's language that the purpose of Rule of Two was to meet established VOSB contracting goals for each fiscal year, holding that if the requirement applied to all VA acquisitions, there would be no need to establish such goals. Because the VA interpreted the statute in a way that gave meaning to the words of the statute, the majority found that the VA's interpretation of the statute was reasonable.

In dissent, Judge Reyna stated that the VA Act does not give the VA discretion to decide whether to conduct a Rule of Two analysis. Noting that the plain language of the Act "unambiguously requires VA contracting officers to conduct a Rule of Two analysis in every acquisition and does not exempt task or delivery orders under the [FSS] from this imperative," Judge Reyna stated that the language regarding the goal-setting purpose was simply prefatory language, and that the operative clause of

the provision requires VA contracting officers to award contracts using the Rule of Two. Judge Reyna also pointed out the impracticality of the majority's ruling, noting that VA contracting officers may not even know the status of the VA's VOSB contracting goals when determining whether to apply the Rule of Two.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our government contracts practice group:

Alan Pemberton	+1.202.662.5642	apemberton@cov.com
Robert Nichols	+1.202.662.5328	rnichols@cov.com
Susan Cassidy	+1.202.662.5348	scassidy@cov.com
Jennifer Plitsch	+1.202.662.5611	jplitsch@cov.com
Steve Shaw	+1.202.662.5343	sshaw@cov.com
Kathy Brown	+1.202.662.5993	kbrown@cov.com
Brian Walsh	+1.202.662.5980	bwalsh@cov.com
Scott Freling	+1.202.662.5244	sfreling@cov.com
Anuj Vohra	+1.202.662.5362	avohra@cov.com
Jade Totman	+1.202.662.5556	jtotman@cov.com
Sarah Liebschutz	+1.202.662.5673	sliebschutz@cov.com