COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

April 16, 2013

THE GOVERNMENT CONTRACTS UPDATE

Covington & Burling LLP's Government Contracts practice delivers an update on major news, notes, and trends relevant to government contractors.

CASE DIGEST

Tolling of FCA's Statute of Limitations During Wartime (*United States ex rel. Carter v. Halliburton Co.*, No. 12-1011 (4th Cir. Mar. 18, 2013))

The United States Court of Appeals for the Fourth Circuit has held that an obscure World War II-era statute—the Wartime Suspension of Limitations Act (WSLA), 18 U.S.C. § 3287[1]—tolls the False Claims Act's (FCA) statute of limitations during times of war. A *qui tam* relator had filed a complaint on June 2, 2011, alleging that Halliburton Company and Kellogg, Brown & Root Services, Inc. (collectively, KBR) had fraudulently billed the U.S. Government for work at U.S. military bases in Iraq from January 2005 through April 2005. Because the complaint was filed after the FCA's six-year statute of limitations expired, the trial court dismissed the suit. On appeal, however, the Fourth Circuit reversed. The Fourth Circuit found that the WSLA still applies to extend the time to pursue fraud actions during wartime to "5 years after the termination of hostilities." The Fourth Circuit held that start of hostilities in Iraq triggered the WSLA's wartime provisions—notwithstanding the absence of a formal declaration of war—and that the WSLA will apply until a Presidential proclamation or Congressional resolution officially concludes the war. Further, the Fourth Circuit held that the WSLA tolls the statute of limitations even when the United States declines to intervene in a *qui tam* action—a curious result given that the WSLA's purpose is to allow *the Government* to bring fraud actions that it lacked the time and resources to pursue while carrying out a war.

This watershed ruling could broadly undermine the FCA's statute of limitations as a bar to untimely fraud allegations. For example, courts now might find that the WSLA tolls the statute of limitations for *any* fraud action against a federal contractor, even if the underlying contract is unrelated to the war effort. In fact, *Carter* already has been cited by a *qui tam* relator alleging false claims for unnecessary medical procedures unrelated to the Iraq war. *See Emanuele v. Medicor Assocs. Inc.*, 10-cv-00245 (W.D. Pa.). Ultimately, although other courts may be hesitant to follow the Fourth Circuit, contractors are well-advised to monitor this trend, as they may find themselves facing decades-old claims of fraud.

NEWS FROM THE HILL

New Cybersecurity Measure Contained in Appropriations Bill

President Obama signed into law a spending bill including a cybersecurity provision designed to curtail what officials describe as a recent surge in Chinese-backed hacking of U.S. businesses. The

[1] The WSLA was enacted in 1942 to extend the time for the Government to pursue actions relating to fraud against the United States during times of war.

spending bill forbids certain agencies—including the Commerce and Justice Departments, NASA, and the National Science Foundation—from using appropriated funds to purchase technology of Chinese origin unless the agency head and the FBI jointly assess the risk of "cyber-espionage or sabotage" and conclude that buying the technology is "in the national interest of the United States."

Notably, this measure applies only through the end of the current fiscal year. However, President Obama's recently unveiled budget proposal for fiscal year 2014 signals that cybersecurity will remain a top priority for the Administration beyond year's end, as it includes billions of dollars for the pursuit of new cybersecurity measures.

Congress Presses Army to Speed Debarment Process:

A group of U.S. senators recently issued a letter expressing "deep concern and frustration" with the Army's delay in debarring companies accused of having ties to Al Qaeda, the Haqqani network, and other terrorist groups. The lawmakers observed that the Special Inspector General for Afghanistan Reconstruction (SIGAR) has referred 43 such companies and individuals to the Army for debarment, but that the Army has yet to take any action. Further, they call on the Army to finalize debarment decisions within 30 days.

This letter is the latest salvo in an ongoing campaign by Congress and SIGAR to speed the Army's debarment process. The Army, which previously has argued that reviewing classified evidence supporting debarment referrals is a time-consuming process that cannot be rushed, has not responded publicly to the letter. As we have previously noted, members of Congress have not been shy about proposing changes to the debarment process, and the senators involved here may well press for new, strengthened debarment measures if the Army does not act quickly to address their concerns.

OTHER NOTEWORTHY ITEMS

FedRAMP Program Criticized for Delays in Certifying Contractors

IT contractors have expressed mounting frustration with back-ups in the General Services Administration's (GSA) Federal Risk and Authorization Management Program (FedRAMP), a centralized, government-wide system for vetting cloud-services contractors. FedRAMP, launched in June 2012, was designed to streamline the security-screening process; an agency could select from a pool of pre-approved contractors for a cloud procurement, as opposed to conducting a separate security review. Nevertheless, the FedRAMP approval process has been painfully slow. To date, just two contractors have been certified.

While many agree that a rigorous screening of cloud providers is critical for data security and privacy, some contractors worry that GSA is ill-equipped to handle the time-intensive vetting process, which has resulted in a bottleneck that only exacerbates approval delays. Further, the slow pace of FedRAMP certification has sparked fears that the program will stifle competition by creating a two-tiered system in which FedRAMP-certified companies enjoy a considerable competitive advantage over IT contractors who, while qualified to do the work, are still awaiting approval. These concerns may well give rise to costly and time-consuming post-award bid protests that could negate the very efficiencies that FedRAMP was designed to promote.

DFARS Amended to Provide Cost Proposal Adequacy Checklist

The Department of Defense (DOD) issued a final rule amending the DFARS to provide a "proposal adequacy checklist" that contractors "should" complete and submit alongside any cost proposal containing certified cost or pricing data. The final rule contains 36 separate checklist items, down from the 47 items included in the initial proposed rule. Found at DFARS 252.215-7009, the checklist is not meant to be punitive, as DOD claims. Rather, it is designed to guide contractors in preparing price proposals, with the ultimate goal of reducing costs and delays associated with rework of noncompliant proposals.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts 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
Steven Shaw	+1.202.662.5343	sshaw@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
Michael Wagner	+1.202.662.5496	mwagner@cov.com