COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

January 6, 2014

THE GOVERNMENT CONTRACTS UPDATE

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

PRESIDENT OBAMA SIGNS 2014 NATIONAL DEFENSE AUTHORIZATION ACT

On December 28, 2013, President Obama signed a compromise version of the FY 2014 National Defense Authorization Act. The law authorizes $527 billion in base defense spending for the current fiscal year, but leaves out a controversial amendment that would remove the decision to prosecute sexual assault cases from the military chain of command. The NDAA contains two procurement-related provisions that are of particular interest to many contractors.

First, Section 937 requires the Secretary of Defense (the "Secretary") to establish a joint software assurance center to "ensure security in the software and hardware developed, acquired, maintained, and used by the Department, pursuant to the trusted defense systems strategy of the Department and supporting policies related to software assurance and supply chain risk management." The Secretary is required to issue a charter for the Center no later than 180 days after the NDAA's enactment. Second, Section 938 requires the Secretary, by March 2014, to supervise the development and implementation of plans for the acquisition of cloud computing capabilities for intelligence, surveillance, and reconnaissance data analysis in the military services and defense agencies. The bill specifically requires that the plans ensure that the cloud systems or services are interoperable and coordinated with the U.S. Intelligence Community. The March 2014 implementation date likely will prove challenging for the Department of Defense ("DOD"). The Senate report accompanying the Act stated that this provision was based in part on recommendations from a Government Accountability Office ("GAO") report, which found that DOD "lacks guidance and standards governing the development of the services' cloud initiatives" and for integrating with the Intelligence Community. GAO also noted that, with the exception of the Army, the remaining services have not yet developed strategies and implementation plans for their intelligence, surveillance, and reconnaissance ("ISR") clouds.

NEW CYBERSECURITY BILL WOULD EXPAND SCOPE OF SAFETY ACT

Last month, Congressman Michael McCaul (R-TX), chair of the House Homeland Security Committee, introduced the National Cybersecurity and Critical Infrastructure Protection Act of 2013. The proposed legislation would, among other things, significantly expand the scope of the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 ("SAFETY Act"), which currently provides liability protection for sellers and users of certain anti-terrorism technologies in the event of a qualifying Act of Terrorism. Section 202 of the bill would expand such liability protections to approved cybersecurity technologies in the event of a qualifying cyber incident.

According to its supporters, the bill would strengthen safeguards against cyber attacks on critical infrastructure while also prohibiting new regulations by the Department of Homeland Security in this

area. Although the proposed expansion of the SAFETY Act in Section 202 of the bill should be welcome news to private industry, several important unresolved questions remain about how the new law would be implemented, including (1) whether the expanded liability protection would apply to technologies already Designated or Certified under the SAFETY Act, and (2) what types of cybersecurity technologies would be eligible for liability protection. The bill has been referred to the Committee on Homeland Security for consideration.

DOD ISSUES NEW INTERIM INSTRUCTION ON ACQUISITION PROCESS

On November 26, 2013, DOD issued an interim instruction intended both to streamline guidelines for the acquisition of goods and account for statutes and regulations passed since the last acquisition instruction was issued in 2008. Unlike its predecessor, the interim instruction does not address the acquisition of services, which will be the subject of a separate instruction expected to be released in the near future.

The interim instruction, which is expected to be finalized by the DOD in 180 days, integrates aspects of DOD's "Better Buying Power" initiative, which includes a set of acquisition principles designed to achieve greater efficiencies through affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition. Significantly for many contractors, the instruction establishes new cybersecurity requirements spread throughout the acquisition cycle. For example, certifications concerning accountability for Information Technology management activities made pursuant to the 2006 Clinger-Cohen Act now require a cybersecurity strategy. The instruction also requires DOD to initiate a "cybersecurity risk management framework" pursuant to the DOD Information Assurance Certification and Accreditation Process ("DIACAP") as early as possible in the acquisition process. Finally, the new instruction requires DOD to institute a cybersecurity strategy for all acquisitions of systems containing information technology. Beyond stating that the DOD Chief Information Officer will review and approve the cybersecurity strategy prior to milestone decisions or contract awards, the instruction provides no further guidance as to the requirements of such a cybersecurity strategy.

DOD ISSUES PROPOSED RULE TO PROTECT AGAINST COUNTERFEITS IN SUPPLY CHAIN

On December 3, 2013, DOD issued a proposed rule that would amend the Federal Acquisition Regulation ("FAR") by requiring agencies to establish procedures to determine the need for more stringent procurement standards to prevent counterfeit products from entering the U.S. government supply chain. The rule follows Section 818 of the National Defense Authorization Act for 2012, which required DOD to issue regulations addressing contractor responsibilities for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect electronic parts. The proposed rule would apply higher standards to products covered by FAR 46.203(b) and (c), which identify items that are "complex" or require "critical applications." The new rule is one of three proposed amendments to the FAR concerning the detection and avoidance of counterfeit parts. (We have previously reported on DOD's efforts to address counterfeit parts in the supply chain.) DOD is also drafting a proposed rule titled "Expanded Reporting of Nonconforming Supplies that would expand the reporting requirements for the use of nonconforming items by contractors.

ADMINISTRATION ANNOUNCES NEW ENERGY EFFICIENCY INITIATIVES

Last month, the Obama Administration recently announced two new initiatives to increase the government's energy efficiency.

The first, announced by the Administration on December 3, extends the 2001 Better Buildings Initiative, which originally required federal agencies to enter into energy savings performance contracts and utility energy services contracts worth at least $2 billion by the end of the 2013. The Administration has not yet set a target for commitments but has said that it will do so in early 2014.

The second, issued via a December 5 executive memorandum, requires federal agencies, by 2020, to utilize renewable sources for at least 20% of their energy consumption "to the extent economically feasible and technically practicable." Agencies will also be required to update energy management practices for their facilities, such as through the addition of energy and water meters. This effort will be phased in beginning in FY 2015, with agencies required to utilize 10% renewable energy sources in that year, followed by 15% in FY 2016 and 2017, 17.5% in FY 2018 and 2019, and 20% in FY 2020 and beyond.

CASE DIGEST

Court Rejects Contractor's Damages Claims, Imposes Penalty for Fraudulent Misrepresentations (*Chapman Law Firm, LPA v. The United States*, No. 09-891 (Nov. 25, 2013))

The United States Court of Federal Claims recently ruled that a contractor had forfeited its claims for costs under a federal government contract and was subject to penalties under the False Claims Act because of misrepresentations it made during performance on that contract. Chapman Law Firm, LPA ("Chapman"), filed suit against the Department of Housing and Urban Development ("HUD") for damages arising from a contract with HUD to provide marketing and management services for homes in Ohio and Michigan. Chapman sought costs related to two stop work orders and modifications to the contract by HUD that Chapman alleged constituted constructive changes. HUD counterclaimed, alleging fourteen violations of the False Claims Act based upon Chapman's submission of four invoices that impliedly—and incorrectly—represented that Chapman had conducted routine inspections of the homes at issue. The court ruled in HUD's favor, holding that the invoices amounted to four separate violations of the False Claims Act and imposed the maximum statutory penalty of $44,000. The court further held that Chapman had forfeited its claims for costs as a result of the Special Plea in Fraud Statute, which provides that "[a] claim against the United States shall be forfeited to the United States by any person who corruptly practices or attempts to practice any fraud against the United States in the proof, statement, establishment, or allowance thereof." The court's holding highlights the severity of the False Claims Act and Special Plea in Fraud Statute.

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
Scott Freling	+1.202.662.5244	sfreling@cov.com
Anuj Vohra	+1.202.662.5362	avohra@cov.com
Jonathan Wakely	+1.202.662.5387	jwakely@cov.com
Jade Totman	+1.202.662.5556	jtotman@cov.com