Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Government Contracts Regulation And Legislation To Watch In 2013

By Dietrich Knauth

Law360, New York (January 01, 2013, 12:00 AM ET) -- With Congress deciding at the last minute to delay the budget cuts in the fiscal cliff, contractors will face a tough legislative and regulatory environment in 2013, squeezed by reduced bottom lines and forced to shoulder more responsibility in areas like cybersecurity, cracking down on counterfeit electronic parts, and fighting human trafficking.

Congress took the fiscal cliff negotiations to the brink, with the Senate and House voting on Jan. 1 to postpone automatic spending cuts and allow the Bush tax cuts to expire for the wealthiest Americans. Though the measure now heads to President Obama's desk, the fiscal drama will likely continue for the first months of 2013, because the deal did not solve the threat of sequestration, nor did it raise the nation's debt limit, which the government will likely hit in February.

Here are some key areas to watch out for in 2013 on the government contracts front.

Sequestration and Defense Budgets

For contractors, no issue has dominated recent conversation quite like sequestration, a series of across-the-board budget cuts set to slash roughly $55 billion from defense and $55 billion from nondefense spending for fiscal year 2013. Sequestration was included in the 2011 Budget Control Act as a doomsday device to spur a future compromise toward deficit reduction, but with Congress unable to come up with an alteriative to the cuts, the “doomsday” scenario is fast approaching.

Just as the calendar turned to 2013, the Senate passed a measure to raise taxes on the wealthiest Americans and delay sequestration for two months, while paying for the delay with a combination of spending cuts and taxes on IRA transfers. During the delay, Congress will continue to negotiate a replacement that lessens the blunt-force blow of sequestration, which leaves little room for agencies to prioritize their spending.

While the fiscal cliff legislation gives Congress more time to negotiate, it also leaves contractors in limbo as they struggle to plan for cuts that may or may not happen.

“Whenever the time comes to make the hard decision, Congress doesn’t make the decision, they keep kicking it down the road,” said Stephan Rice of Crowell & Moring LLP. “The uncertainty of sequestration is still looming out there, so for contractors, the deal that was struck yesterday doesn’t resolve a lot for them.”

Sequestration will not impact already-funded contracts, but it will cut down on unobligated funds and reduce the amount of money available to extend programs and start new projects. Agencies will be forced to prioritize their contracts as much as they can within the rigid constraints of sequestration, and contractors should look for vulnerabilities and plan for the worst.

“At one point, there were 17 unmanned aerial vehicle programs across the [U.S.] Department of Defense. ... In that kind of environment, they're going to have to choose between competing programs, they're not going to be able to afford all of them,” said Jim Schweiter, a partner with McKenna Long & Aldridge LLP.

The government will also seek to shift to fixed-price contracts and away from cost-reimbursement contracts and time and materials contracts, while looking to terminate contracts that aren't giving the government the kind of return it wants. The government could also buy fewer drones and warships, while stripping away equipment add-ons or services it can no longer afford, opting for a “a Chevrolet capability instead of a Cadillac capability,” according to Schweiter.

Appropriations Bills

Beyond sequestration, contractors and must deal with the continued uncertainty about federal funding levels after living with more than a year and a half of short-term budgets. The current omnibus appropriations bill funds the government through April, and contractors could also be caught up in the threat of a government shutdown during a possible sequel to 2011's deficit ceiling battle. The government is likely to reach its borrowing limit in February, and Republican lawmakers have already threatened to hold the debt ceiling hostage to extract more spending cuts.

That approach could have a negative long-term impact on federal budgeting, threatening to turn the debt ceiling into a permanent weapon that the minority party in Congress can use to stymie laws and budgets they disagree with, according to Rice.

“I think the arguments about the debt ceiling are disingenuous at best, because raising the debt ceiling only allows the government to honor the debts that are already appropriated and authorized by Congress,” Rice said. “That isn't a partisan issue. It's problematic that it's starting to creep into and hold hostage these other bills that Congress needs to get to.”

The congressional gridlock has kept agencies and contractors stuck in a holding pattern of short-term spending bills that don't allow agencies to invest or commit resources to tackling new or challenging problems, Rice said.

Whatever happens, budgets are due for a decline, and contracting costs, which tripled during the eight years of George W. Bush's presidency before declining slightly under the Obama administration, are a prime target for cuts.

“Contractors really need to think beyond the cliff,” said Rich Rector, head of DLA Piper's government contracts group. “Whether or not there's a cliff, there's definitely a valley coming, in terms of spending.”

National Defense Authorization Act

The 2013 National Defense Authorization Act will bring new challenges and costs for contractors, and it includes several provisions aimed at reforming the way the DOD buys weapons and services.

The NDAA includes a last-minute amendment added by Senate Armed Services Committee Chairman Carl Levin, D-Mich., which requires cleared contractors to report on cyberattacks and grant DOD access to information systems for security checks. Contractors complained that the amendment's initial language would have provided the DOD with open-ended access to data — even to the point of long-term confiscation of computer servers — with very little controls on how that information would be used or safeguarded.

While the final version of the NDAA limits the amendment in a few key ways, requiring the DOD to safeguard trade secrets and commercial information and preventing the DOD from sharing the information outside of the agency, it doesn't go far enough, according to Elizabeth Ferrell, a partner in McKenna Long & Aldridge LLP's government contracts practice.

"It's a good first step, but it doesn't resolve all the issues," Ferrell said.

The new language clarifies that contractors only need to provide enough access to allow the DOD to determine the extent to which its data is breached, but it still doesn't limit the DOD's use of that information once it's obtained and doesn't address contractors' concerns about wholesale copying of data or seizure of computers.

The NDAA also includes wartime contract reform legislation authored by Sen. Claire McCaskill, D-Mo., who initially introduced her bill as separate legislation before offering it as an amendment to the NDAA. McCaskill's amendment is based on the recommendations of the bipartisan Commission on Wartime Contracting, which was created through legislation McCaskill co-authored with retiring Sen. Jim Webb, D-Va.

Under the wartime contracting reforms amendment, contractors indicted or accused of felonies would automatically be referred to suspension and debarment authorities, and it would require agencies to issue periodic reports on the number of open suspension and debarment cases in an effort to prod agencies to move faster. The amendment also includes enhanced whistleblower protections for nondefense contractor employees.

A lesser-noticed provision in the NDAA prohibits the DOD from using cost-reimbursement contracts for major weapons programs. While some observers see the change as cosmetic, because the DOD can get around it with a certification from the undersecretary of defense for acquisition technology and logistics, Schweiter said that it sends a clear message that the government is seeking to push more financial risk towards contractors when developing new weapons.

Historically, cost-reimbursement contracts have been used for new and hard-to-budget projects that involve significant research and testing costs. The new legal language implies a higher level of congressional scrutiny and an effort to cap such costs early on, which may not be practical, Schweiter said, given the recent experiences with programs like the Lockheed Martin Corp.-designed F-35 Joint Strike Fighter, which proved more expensive than initially planned as developers struggled to incorporate stealth, supersonic speed, advanced computers and heavy weapons systems into a single, all-purpose aircraft.

"That really is a fundamental sea change in these types of acquisitions," Schweiter said. "As a policy statement, to me, that's a significant step even if you can overcome it with a certification."

Among the changes that were removed from the final bill were a provision that would have empowered the Defense Contracting Audit Agency to access contractors' internal audits, required inflexible cuts to the DOD contractor and civilian employee workforce, and sharply reduced the amount that the government will pay towards contractor executive salaries.

In addition, the legislation makes strides towards removing export restrictions on commercial satellites, and does not include two House amendments that would have prevented the U.S. military from investing in biofuels, which the military — the Navy in particular — has pursued to shield itself from volatility and scarcity in oil markets.

The NDAA also includes a provision that could ease contractor concerns about still-pending DOD regulations on counterfeit electronic parts. The 2013 NDAA would allow contractors to bill the government for some costs related to identifying, removing and replacing counterfeit electronics if they rely on a trusted supplier, have adequate screening processes and provide timely notice to the government.

Counterfeit Electronic Parts

While the new NDAA addresses some contractor concerns about the allowability of costs, the DOD's forthcoming rules on counterfeit parts still carry significant ramifications for defense contractors. The new rules have contractors bracing for a wide range of inevitable new costs, from new screening and compliance processes to dealing with a shrinking and more expensive supplier base.

The law leaves open many questions about contractors' exact responsibilities, including the definition of "suspect counterfeit" parts and the kinds of compliance and vetting that the DOD will accept, leaving contractors to wait on the DOD's implementing regulations to get a better picture of the kinds of costs and policy changes they'll face.

"The counterfeit parts issue is sure to remain a hot topic for government contractors in 2013," said Craig Holman, a partner at Arnold & Porter LLP who co-wrote an American Bar Association white paper on the topic.

The military faces the highest risk for counterfeits when it tries to buy outdated parts to extend the life cycle of older weapons systems, and when it tries to rely on commercial, off-the-shelf items, attorneys say. Both approaches typically save money for the DOD, but the new anti-counterfeiting rules will likely blunt those savings by requiring more expensive vetting of suppliers and testing of potentially suspect parts.

Despite higher costs, the government is likely to continue to push for more vetting, because the risks, as shown by two 2012 congressional reports, include major system failures and back-door access that facilitates espionage, according to Holly Roth, a partner at Manatt Phelps & Phillips LLP.

"Some of those products actually have bugs in them and listening devices, so at one end of the extreme, counterfeit products could actually assist a foreign national — an unfriendly foreign national — to spy on the U.S. government," Roth said.

Cybersecurity

While Independent Connecticut Sen. Joe Lieberman's Cybersecurity Act died on the Senate floor in 2012, contractors expect Congress to try to tackle the issue again in 2013, as data security remains a significant vulnerability for the government.

Congress would likely move on a "watered-down" version of the failed Lieberman bill, giving new authority to the U.S. Department of Homeland Security and establishing a process to allow the government and private companies, including contractors who host federal data and owners of critical infrastructure like power grids, to share real-time information about cyberthreats, according to Robert Nichols, head of the government contracts group at Covington & Burling LLP.

A new cybersecurity bill would have to draw lines on when companies are required to report cyberbreaches, and would likely give contractors some protection from litigation arising from those reports, but where those lines are drawn is anyone's guess, Nichols said.

While Congress works on a new bill, the White House is likely to push a cybersecurity executive order to fill the gap, and agencies will pursue ad hoc cybersecurity efforts through their own regulatory authority or through contract provisions. One of several pending rules aimed at safeguarding the government's data will likely be finalized in 2013, according to Peter Eyre of Crowell & Moring LLP.

“I think there is enough pressure and enough scrutiny that we will see a final rule. It may be one of these rules and it may be a hybrid, but I think we will see something,” Eyre said. “At a moment where there is not a particular standard, this is something that contractors will need to keep a close eye on, because it could have wide-ranging impacts.”

While many contractors focus on the expense and burden of new cybersecurity rules, Anuj Vohra of Covington said that contractors could actually have a chance to shape the current debate to their advantage, by helping shape what future cybersecurity requirements will look like.

“Our thinking is that this is actually very important for contractors to be weighing in on what the laws and regulations will say, not only to relieve themselves of excess administrative burdens, but also to position themselves more strategically for future acquisitions,” Vohra said.

Human Trafficking Regulations

A recent White House executive order recruits federal contractors in U.S. efforts to fight labor trafficking at home and abroad, giving contractors increased responsibility to report, root out and remedy labor trafficking among their subcontractors and labor recruiters.

The order's impact will depend on the regulations written to carry it out, but the order requires contractors to certify that neither they nor any of their contractors have engaged in trafficking-related activities, and bans the use of recruitment fees in exchange for the promise of work, a common tactic for companies engaged in trafficking.

The executive order also forbids companies from misleading potential employees about the locations of their jobs, lying about living and working conditions, denying them access to their passports or drivers' licenses, or failing to pay return transportation costs for employees who travel to other countries for work. Contractors must also train employees to spot signs of trafficking and allow them to report trafficking violations without fear of retaliation.

The human trafficking rules take a similar approach to the counterfeit electronics rules, requiring much more diligence from contractors in policing their suppliers and companies they work with, according to Eyre.

“That is a trend,” Eyre said. “The government isn't just buying services; it is also trying to achieve certain policies and principles.”

In addition combating the moral problem of trafficking, a zero-tolerance also reduces security risks at U.S. facilities, because apparent tolerance for trafficking breeds ill will, and trafficked workers could be recruited by terrorists, Roth said.

“Where people believe they're being subjugated, they're going to look for a way out or recourse, and that recourse won't be pleasant, particularly if they believe that the U.S. government is somehow approving of those activities,”Roth said.

--Editing by Elizabeth Bowen.