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 2014

By **Dietrich Knauth**

Law360, New York (January 01, 2014, 10:08 AM ET) -- The two-year budget deal signed at the end of 2013 offers at least a pause in the budgetary brinksmanship that led to the haphazard budget cuts of sequestration and a 16-day government shutdown, but Congress will force contractors in 2014 to think on their feet as lawmakers seek to address embarrassing procurement missteps, such as the early failures of HealthCare.gov, and leverage the power of the purse to pursue social and political goals.

Here are the areas to watch for additional legislation and regulation in 2014:

Information technology procurement reform

The botched rollout of HealthCare.gov ramped up scrutiny of the federal information technology acquisition process, prompting calls for change in 2014 amid a growing consensus that the way the government buys technology is too slow, too burdened by inefficiencies and too prone to high-profile failures.

The legislation with the most momentum behind it, Darrell Issa's, R-Calif., Federal Information Technology Acquisition Reform Act, suffered a setback when it was removed from the National Defense Authorization Act, the must-pass legislation that authorizes defense spending, in December. FITARA was included in the version of the NDAA that passed the House in June, and offered as an amendment to the Senate NDAA, but it was removed in a last-minute rewrite of the law aimed at quickly passing the bill after the Senate ran short on time for amendments and debate.

Still, FITARA, or legislation like it, remains on Congress's agenda in 2014, and it could mitigate some of the persistent problems with IT purchases by giving more budget authority and responsibility to agency chief information officers, creating a streamlined approval process for new information technology contracts, and redirecting money from existing contract management funds to fund IT training for the government's acquisition personnel.

Contractors generally see empowering CIOs as a good step toward fixing some of the dysfunction that plagues IT procurement, according to Alan Pemberton, co-chair of the government contracts group at Covington & Burling LLP. Contractors would rather directly “talk to the people who actually know the technical aspects of the system and can make sure that the right types of systems are being bought,” rather than have the CIO sidelined by budget and acquisition people who are less familiar with the technology requirements in a procurement.

Though FITARA's reforms would help, anyone who suggests that they'd solve the problems behind the troubled rollout of online health insurance exchanges is kidding themselves, according to Alan Chvotkin, general counsel for the Professional Services Council.

"It's not a perfect bill. It has elements that are helpful, such as clarifying the role of CIOs, that are long overdue, and if the Congress passes it, it will contribute to some of the issues," Chvotkin said. "It is not a solution for HealthCare.gov, and if it's being talked about as ensuring that another HealthCare.gov will never happen, I think that oversells what FITARA is capable of doing."

Suspension and debarment

Suspension and debarment is an increasingly popular topic in Congress, and that won't change in 2014, as lawmakers seek to prevent taxpayer dollars from flowing to companies with questionable ethics or track records.

Congress has proposed a more comprehensive overhaul of the government's approach to suspension and debarment through the Stop Unworthy Spending Act, or SUSPEND Act. That bill would create a new governmentwide suspension and debarment board, and allow some civilian agencies and the U.S. Department of Defense to opt out of the planned consolidation if they can demonstrate that they already have strong suspension and debarment offices.

The waiver option could help civilian agencies with relatively sophisticated suspension and debarment programs, such as the U.S. Environmental Protection Agency, maintain control of their programs, and would treat the DOD and military services just like any other executive branch agency. That change has alleviated some criticism of the bill and turned some early skeptics into cautious supporters.

Congress has ramped up its scrutiny of contractor suspension and debarment in recent years, after reports by the U.S. Government Accountability Office and the Commission on Wartime Contracting highlighted weaknesses in the suspension and debarment offices of civilian agencies. The SUSPEND Act was proposed after oversight hearings embarrassed some agencies that rarely suspended or debarred any contractors.

Beyond the obvious impact of taking suspension and debarment authority away from some agencies, passing the SUSPEND Act would likely lead to more of a litigation-style approach to suspension and debarment, according to Frederic Levy of McKenna Long & Aldridge LLP.

"The rules for responsibility will stay the same," Levy said. "The process by which it is determined is going to be much more formal, much more rigorous, and with public decisions you're going to see more and more of a litigation bar arising around suspension and debarment."

Though the SUSPEND Act is the most dramatic change that's on the table, it is likely that Congress will also pursue piecemeal additions to the range of offenses that result in automatic debarment, according to David Robbins, a former Air Force debarring attorney who now heads the government contracts practice at Shulman Rogers Gandal Pordy & Ecker PA.

The rise in automatic debarments puts government agencies and their contractors in a tight spot, Robbins said, because the automatic exclusions are a slippery slope, and lingering debarments with no agency discretion would "absolutely ruin everyone's ability to get anything done.

"The solution to every problem cannot be to eliminate companies from competition," Robbins said. "There has to be something short of the 'death penalty' of suspension and debarment."

Supply chain management

Rules proposed in 2013 have required contractors to make significantly greater efforts to police their supply chain and their subcontractors for counterfeit electronic parts and evidence of human trafficking. Those rules could be finalized in 2014, and attorneys expect the focus on supply chain scrutiny will spread to other areas, opening up new risks and potential liabilities.

"I think there's going to be much more focus on sources and how prime contractors supervise and monitor subcontractors in their supply chain," said Peter Eyre, an attorney with Crowell & Moring LLP. "This is an area that is changing quite rapidly."

Visibility into a company's supply chain will cost money, requiring negotiations with subcontractors, pushback and new agreements.

"There's also a question of who's going to bear those costs," Eyre said. "There are dollars associated with closer scrutiny of the supply chain."

The government advanced significant rules on counterfeit electronic parts and human trafficking in 2013, taking the same approach to pursue very different goals. In the counterfeit parts rule, the DOD will evaluate contractors' efforts to scour its supply lines for counterfeit electronics — which pose greater risk of failure and sabotage — as part of its review of contractor purchasing systems. In the human trafficking rule, proposed in September, the government will require contractors to police subcontractors and recruiters for telltale signs of worker exploitation, such as confiscating passports and charging recruitment fees.

An interim rule issued on Nov. 18 expands the same kind of oversight responsibilities to information technology components sold for use in national security systems. That rule is especially noteworthy for contractors, because it gives the DOD the ability to exclude IT contractors from a contract competition if the DOD determines that a contractor or subcontractor presents a supply chain risk, without requiring a full explanation, according to Susan Cassidy of Covington & Burling LLP.

"You can be excluded from a procurement, and there's a provision that DOD can limit disclosure of why, so you may not even know why," Cassidy said. "Just from a practical standpoint, this could put contractors in a terrific bind."

Cybersecurity

Protecting the government's data will remain a focus for federal agencies and their contractors in 2014, and experts expect more regulation in support of that goal.

"The government is broadening the definition of protected data," Eyre said. "It's no longer just classified information, it's not just technical data under ITAR, it's more generally protecting contractor networks that contain government data."

Late in 2013, the government finalized a rule requiring contractors to take additional steps to safeguard unclassified technical data, paring down a cybersecurity rule that was criticized as being too broad when

proposed in 2011. Though the 2011 proposed rule would have required enhanced cybersecurity for a broader range of unclassified information provided by or developed for the DOD, the final rule is limited to unclassified technical documents related to DOD-funded research and development — including computer software and documents such as engineering drawings, technical manuals, blueprints, data sets, studies and analyses — and to other technical information that could be used to produce, repair or modify any military or space equipment.

The new rule requires contractors to take enhanced cybersecurity measures to protect DOD technical data. The cybersecurity measures are drawn from commonly used practices codified by the National Institute of Standards and Technology, including access control, awareness and training, contingency planning and maintenance.

Some concerns remain for contractors, including the lack of a safe harbor for contractors who report breaches despite complying with the NIST standards, and some ambiguity in the definition of a cyberevent that must be reported, according to Elizabeth Ferrell of McKenna Long & Aldridge LLP.

"Even though they've really narrowed this down, there are certain things that are still troubling from a contractor's perspective," Ferrell said.

The DOD said in the final rule that reported cyberincidents will not, by themselves, be considered evidence that a contractor had inadequate security, but flatly denied any safe harbor requests in the comments to the proposed rule, saying "the government does not intend to provide any safe harbor statements."

Though the DOD has said that the cyberincident reports will not be disclosed as a result of Freedom of Information Act requests, contractors are wary about ways the reports could be used against them, such as impacting their performance reviews or disqualifying them from contract competitions under the supply chain rule, Cassidy said.

"There's a requirement to report, but it's unclear what DOD's going to do with that information," Cassidy said.

--Editing by Stephen Berg.
