

Gov't Contracts Legislation And Regulation To Watch In 2015

By Erica Teichert

Law360, Washington (January 02, 2015, 3:23 PM ET) -- Although Congress signed off on the \$585 billion defense spending bill in the last week of its lame-duck session and agencies released some long-awaited rules in December, government contractors will be eagerly awaiting updates from regulators and legislators on a slew of issues in 2015, such as sexual harassment reporting requirements, supply chain management and cybersecurity rules.

Here is some of regulation and legislation government contractors are homing in on this year.

Labor and Employment Rulemaking

The U.S. Department of Defense, General Services Administration and NASA closed out 2014 by **issuing** some interim rules on government contracting matters, including one that implemented President Barack Obama's February directive to raise the minimum-wage rate for workers on federal contracts to \$10.10 per hour, starting on Thursday.

While that rule and other related standards from the feds have already sparked some debate, government contractors are still waiting to weigh in on several other potentially controversial statutes.

According to several government contracts attorneys, the industry is particularly concerned with the implementation of two Obama executive orders that will require government contractors to divulge adverse merits determinations on a variety of employment issues. These include wage-and-hour violations under the Fair Labor Standards Act, discrimination under Title VII of the Civil Rights Act of 1964 and unfair labor practices under the National Labor Relations Act.

Government contractors don't yet know the extent of the proposed disclosure requirements. Covington & Burling LLP's Jeff Bozman said the executive order envisioned reporting requirements for serious, repeated, willful or pervasive employment violations but left the requirements themselves relatively vague. The eventual rules could create a burden for companies, he said.

"One of the concerns there is with the serious and willful prongs of that test," he told Law360. "In theory, those could require disclosure for a single act if it was serious enough or willful enough. Repeated or pervasive seem to imply some sort of pattern of misconduct. The serious and willful prongs will certainly deserve close attention when those proposed regulations come up."

Crowell & Moring LLP's Peter Eyre noted that no proposed rulemaking has stemmed from that executive order yet, and there's no word on the time frame for the rules' release. At the moment, there's talk that the employment-related disclosure rules won't go into effect until 2016, but many issues are still up in the air, he said.

Government contractors are also watching out for employment-related guidance from the Hill, according to Wiley Rein LLP's Scott McCaleb. In particular, the Restore Opportunity, Strengthen and Improve the Economy Act, H.R. 5250, could prevent some companies from receiving government contracts if they don't provide workers with a living wage, benefits or paid leave.

"This is kind of another run at the Clinton blacklisting rules from the end of the Clinton administration, where they're basically trying to penalize contractors with various labor and employment violations based on their record of compliance with those sorts of laws, as evaluated and administered by contracting officers," McCaleb said.

Dueling Cybersecurity Reporting Requirements

Cybersecurity remains a key issue for government contractors in 2015, as the DOD, the National Institute of Standards and Technology and other regulators still have cybersecurity guidelines they need to promulgate.

Although the DOD issued a final rule in November 2013 on protecting and safeguarding unclassified controlled technical information, it's the only final cybersecurity rule of this nature for defense contractors so far, and companies can expect to have multiple, overlapping standards from the various agencies they work with. While the DOD will expect some information on a cyberbreach affecting UCTI within 72 hours, other agencies could expect more extensive information in a shorter timeframe.

"They're going to have to figure out a way to know when to report, what to report, who to report it to, and they're going to have to have a way to monitor all of their information systems and networks to make sure they're catching all these incidents," Covington's Catlin Meade told Law360.

While the DOD's final rule on safeguarding UCTI includes 51 specified security controls, the agency and other regulators are also promulgating guidances on what to do after a hacker has breached a contractor's system.

So far, the Nuclear Regulatory Commission is the only agency that has released a comprehensive draft rule providing nuclear reactors with cybersecurity requirements on what data needs to be reported within an hour, four hours, eight hours and 24 hours after an attack or before an imminent attack.

"Although it's different from the defense contracts and the intelligence communities, and it's technically not geared toward contractors, it would be interesting if others use this as an example," Meade said.

Under the 2013 National Defense Authorization Act, the DOD was required to impose rapid reporting requirements on contractors within 90 days, but those rules still haven't come out after repeated delays.

Meanwhile, NIST issued a draft publication of a number of security controls in November 2014 that would apply to any contractor that proffers, stores or transmits controlled unclassified information on its own systems.

Contractors that work with multiple agencies could become overburdened by trying to comply with so many conflicting reporting requirements, and they will likely have to overhaul their entire cybersecurity and reporting framework to meet the toughest system.

"It's very likely this will apply to their network as a whole," Meade said. "They're going to have to look at what their contracts impose on them and what's the highest level of security they will have to impose. That's kind of being lost on people."

Tighter Controls for Contractors and Tax Inversion

Just last month, the DOD, the GSA and NASA came out with an interim rule updating the prohibition on inverted domestic companies or their subsidiaries receiving government funds for contracts. The latest revision sought to make it more clear which corporations are covered by the law.

The interim rule deleted what it said was "a long listing of exceptions that ... had become increasingly difficult to understand with the passage of each appropriations act." It replaced this laundry list with the statement that the rule "shall not apply to any federal government contract entered into before the date of the enactment of the act, or to any task order issued pursuant to such contract."

While the interim rule hasn't changed the definition of an inverted domestic company, the latest regulation makes clear that the government is taking a closer look at the ban, according to Covington's Mike Wagner and Jennifer Plitsch. The agencies simultaneously issued a proposed rule that requires contractors to complete a two-step checklist certification showing they are not an inverted domestic corporation and to provide contracting officers with written notification if their inverted status changes.

"It is yet another signal of the government's intention to tighten restrictions on companies that redomicile abroad for tax purposes," Plitsch and Wagner said. "The proposed rule leaves open some real questions about how it would be implemented in practice, but the thrust of the rule is certainly consistent with the trend toward greater emphasis on inversion issues."

Wagner said the revisions may not end there, as both the U.S. House of Representatives and Senate have proposed bills that would expand the definition of an inverted government contractor.

Currently, a company is considered an inverted domestic corporation if 80 percent of its stock is held by former shareholders of the original domestic company. But under the No Federal Contracts for Corporate Deserters Act of 2014, S. 2704 and H.R. 5278, that threshold will go down to 50 percent. Wagner noted that the bill would also prevent inverted companies from becoming top subcontractors.

"Lowering that continuity threshold would be a big deal," Wagner said.

Thanks to the combined regulatory and legislative efforts, Wagner and Plitsch said it's clear that anti-inversion issues will remain a hot topic this year.

"It remains to be seen whether any of these specific bills will be adopted, but these rulemaking actions show that the issue has staying power beyond the election cycle," they said.

Supply Chain Management

Regulators issued several supply chain management-related rules in 2014, and that area remains a hot

topic for government contractors this year. While the DOD has already released final rules in areas such as counterfeit parts in recent months, some anticipated guidances, including an anti-human trafficking regulation, are still under wraps.

The Federal Acquisition Regulatory Council, made up of the DOD, GSA and NASA, issued a proposed rule in June that would require contractors to report suspected counterfeit or defective parts to a central government clearinghouse known as the Government-Industry Data Exchange Program and to check with GIDEP's database before purchasing parts.

The rule builds on a narrower rule that was finalized in May, which affects only DOD contractors and addresses reporting only for electronic parts that are intentionally counterfeited.

Contractors have already been fighting back against the expanded reporting requirements, criticizing the proposal for lacking specificity and ignoring some practical stumbling blocks. The expansions would be a significant change for companies, and the unpolished definitions have some concerned about how contractors will know exactly what they need to report.

"There are going to be new requirements to monitor," Eyre said.

Obama also signed an order in 2012 that will recruit 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. But so far, the anti-human trafficking rule has stayed under wraps.

"That proposal came out months ago," Eyre said. "That is now, as far as we can tell, ready to come out in final form. Because of the compliance requirements of that rule, it's something that will get a lot of attention."

GSA Schedule Issues

Eyre said government contractors are expecting the GSA to consolidate some of its service schedules and promulgate new disclosure requirements, both of which could mean changes for the industry.

In particular, the GSA has signaled that it will consolidate its schedules involving consulting and information technology services in an effort to promote efficiency and snag better deals for the services it purchases. And with so many contractors involved in those massive schedules, the move is sure to pique companies' interest.

"That signal has been given to industry, but the devil is in the details," Eyre said.

The GSA has made other pushes for increased efficiency in past years, including launching a website for reverse auctions in July 2013 to save money and improve small business opportunities by making it easier for contractors to compete to provide office supplies and commercial IT to the government.

The agency is also considering establishing additional disclosure requirements for contractors on GSA schedules that could provide the government with discounts if other customers pay less than a benchmark price for the same services.

"There's discussion around trying to streamline those requirements, but there's nothing concrete yet,"

Eyre said. "Because of the volume of companies on these schedules, it's something that a lot of people are watching."

--Additional reporting by Khadijah M. Britton. Editing by Kat Laskowski and Katherine Rautenberg.

All Content © 2003-2015, Portfolio Media, Inc.