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

Self-Reporting Is All The Rage In Recent Contractor Regs

By **Dietrich Knauth**

Law360, New York (August 25, 2014, 6:00 PM ET) -- From False Claims Act violations to cybersecurity breaches to labor violations, self-reporting requirements are making a huge splash upon the regulatory scene, and experts say it is becoming ever more difficult for contractors to keep pace with expanding disclosure requirements.

The recent trend kicked off with the 2008 mandatory-disclosure rule covering fraud and False Claims Act violations, but it has picked up in the past year, with a flurry of new requirements being driven by executive orders on cybersecurity, human trafficking and labor law enforcement.

“In the last eight months, the number of things you need to self-report seems to be growing exponentially,” said Susan Cassidy of Covington & Burling LLP. “It really is just an explosion of new requirements that contractors are desperately trying to catch up with.”

Not all of the new rules are created equal — some are aimed more at prevention while others aim at enforcing compliance, and some require much more legal analysis from contractors than others. But all carry compliance costs and risks for contractors, attorneys say.

“It's attractive to the government to think they're going to get all this reporting and compliance and internal controls, but they don't necessarily come for free,” said Kara Sacilotto, a partner with Wiley Rein LLP.

While it may be less expensive for the government to rely on self-reporting rather than hiring more overseers and investigators, some of the costs will inevitably end up being borne by the government, according to David Hammond, a partner at Crowell & Moring LLP.

“It's going to cost the government to review these disclosures,” Hammond said. “It's going to drive up the contractors' costs of compliance ... and that is going to result in higher indirect costs being charged to the government."

The plethora of rules could also drive come companies out of the government contracting business, potentially causing prices to rise as a result of lessened competition, Hammond said.

The proliferation of disclosure and self-reporting regulations carry significant risks and uncertainties for contractors, especially in light of the lack of uniformity among the rules, Sacilotto said. Each requires a different level of legal analysis, different subject-matter expertise and varying standards for when

contractors must make disclosures.

“One of the things that makes it pretty challenging is that the standards aren't the same,” Sacilotto said. “For example the FAR mandatory disclosure rule has a requirement for 'credible evidence' of misconduct, but the human-trafficking rule has a different standard in the statute, and the Anti-Kickback Act has a different standard. If I'm a contractor, I have all of these different standards, and my compliance program needs to make sure that it covers all of these different standards.”

Based on the government's recent experience with the mandatory-disclosure rule for fraud and FCA violations, and the political interest in advancing policy goals through contracting, additional rules are likely to expand the number of violations and incidents that contractors are forced to self-report, Hammond said.

“The number of disclosures may reinforce policymakers' views that there are more violations out there than they could ever know about, and that we should expand the scope of such mandatory disclosures, but the data may be skewed in that many companies, especially large companies, have policies that disclose everything, even very minor ones," Hammond said.

With all the unique risks and challenges that come with self-reporting, here are five self-reporting obligations for contractors to keep in mind:

Mandatory Disclosures of Fraud

The current disclosure trend can be traced back to the 2008 finalization of a Federal Acquisition Regulation rule requiring contractors to disclose “credible evidence” of fraud, significant overpayments or False Claims Act violations to their agency inspector general.

”It's fair to say that the mandatory-disclosure requirement was a watershed event,” Sacilotto said.

The FAR mandatory-disclosure rule, while the most developed of current self-reporting regulations, still gives contractors headaches, in part because of the legal judgment necessary to determine when a contractor has “credible evidence” and because of the varying enforcement approaches taken by different inspectors general.

“Determining whether you need to make a disclosure can be legally complex, factually complex,” Sacilotto said. “You have to understand the legal nuances of the False Claims Act to make that decision.”

The rule, while still somewhat rough around the edges, has paved the way for future self-disclosure rules.

"The mandatory-disclosure rule, which was controversial when passed, was the camel's nose in the tent. Now that contractors have accepted that and have been complying, there's less resistance to adding more disclosure obligations on top of it," Hammond said.

The Federal Awardee Performance Integrity Information System

The Federal Awardee Performance Integrity Information System, created in 2010 and made public in 2011, acts as a clearinghouse for contractor responsibility information, aiming to give government contracting officers a single-source database for assessing contractors' level of integrity, past

performance and responsibility.

Under FAPIIS regulations, contractors are required to self-report criminal convictions, civil liability and administrative proceedings related to the performance of government contracts, if those proceedings resulted in a finding of fault and the contractor paid $5,000 or more in damages, restitution or fines. Those disclosures, while more clear-cut than the earlier mandatory-disclosure rule, still offer plenty of risk for companies, attorneys say, citing increased exposure to bid protests and other litigation including False Claims Act suits

Counterfeit and Nonconforming Parts

In addition to using self-disclosure to increase compliance, Congress and the executive branch have also pushed new reporting requirements as a way to proactively protect the government from the risks associated with counterfeit electronic parts. Defense contractors are already starting to adjust to a May 2014 final rule on counterfeit electronic parts, and the Federal Acquisition Regulatory Council agencies are weighing a separate proposal that would significantly expand anti-counterfeiting responsibilities for all government contractors and greatly expand the government's database of suspected counterfeit or nonconforming goods.

The DOD rule, proposed in May 2013 to implement a provision in the 2012 National Defense Authorization Act, requires defense contractors to scour their supply lines for counterfeit electronics, which pose greater risk of failure and sabotage, and it puts contractors on the hook for the costs of replacing any counterfeits that make their way into DOD weapons systems. Contractors have worried that the regulation will cause financial harm and that expensive anti-counterfeit testing and vetting procedures will force some companies out of the DOD supply chain entirely.

In addition to the DOD rule, the government is weighing a far broader change to the Federal Acquisition Regulation. While the previous rule applies only to the DOD, only to electronic products and only to intentional counterfeits, the FAR rule, proposed in June 2014, would cover all contracts and extend to nonelectronic counterfeits and noncounterfeit but defective parts.

In both the DOD final rule and the proposed FAR rule, contractors are required to report counterfeit parts to a central government clearinghouse known as the Government-Industry Data Exchange Program and to check GIDEP's database before purchasing parts.

Cybersecurity Breaches

Like counterfeit electronics, data breaches are another area where the government is using contractor reporting as a form of proactive protection. Late in 2013, the government finalized a rule requiring contractors to take additional steps to safeguard unclassified technical data that could be used to produce, repair or modify any military or space equipment. The rule covers computer software, engineering drawings, technical manuals, blueprints, data sets, studies and analyses, and other technical information

The new rule requires contractors to take enhanced cybersecurity measures to protect DOD technical data, drawing on commonly used practices codified by the National Institute of Standards and Technology, including access control, awareness and training, contingency planning and maintenance. The rules require quick reporting of any breach that could impact unclassified controlled technical information.

Contractors are still waiting on other cybersecurity rules, including separate “rapid reporting” requirements that will apply to DOD and intelligence community contractors with access to classified information. The DOD has proposed a 72-hour window for reporting sensitive data breaches, while the intelligence agencies, whose rapid reporting mandate was only signed into law in July 2014, have yet to propose a timeline.

Labor Violations

The most recent self-reporting requirement, established by executive order on July 31, is also one of the broadest, requiring contractors to report a whole host of labor violations to the federal government, including wage-and-hour violations under the Fair Labor Standards Act, discrimination under Title VII of the Civil Rights Act of 1964, unfair labor practices that violate the National Labor Relations Act, and leave violations under the Family and Medical Leave Act.

Because the executive order requires the reporting of violations and judgments, it shouldn’t require the kind of thorough legal analysis required by the FCA mandatory-disclosure rule or the rapid-fire reporting required by the cybersecurity rules, according to Sacilotto. In that way, it isn't so different from the FAPIIS reporting requirements, she added.

On the other hand, attorneys say that the rule will require significant changes — and significant investments — from both the government and its contractors and that it raises many questions about implementation to be ironed out as regulations develop. The order could also incentivize companies to settle labor disputes rather than risk losing a case and triggering the reporting requirement, according to Connie Bertram of Proskauer Rose LLP.

The recent executive order also builds on a previous order aimed at combating labor violations abroad. President Barack Obama 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.

Contractors have some time to adjust to the newest requirements, since no regulations have yet been formally proposed, and the July 31 executive order says that the requirements will take effect in January 2016.

The order also leaves open the possibility that other reporting requirements could piggyback on some of the new structures put in place for the labor reporting, including a new federal database “for all federal contract reporting requirements related to this order, as well as any other federal contract reporting requirements to the extent practicable.”

--Editing by Jeremy Barker and Chris Yates.
