DFARS Cyber Compliance And Potential For FCA Risk

December 18, 2017
By Colleen Brown, Robert Conlan and Christopher Fonzone

For well over a year, defense contractors have had New Year's Eve 2017 circled on their calendars, and not because they love the "auld lang syne" and a good glass of champagne. (Or at least not only for those reasons.) Dec. 31, 2017, is the deadline for when covered contractors must comply with the U.S. Department of Defense's new Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirements. This holiday season contractors are thus making their lists and checking them twice in order to ensure that they will be compliant by the end of the year. And this intense focus is well warranted. The DOD is deeply committed to protecting its information, and the requirements are an important step in that regard.

But for all of the focus on Dec. 31, contractors must also remember that the focus on compliance must remain into the New Year — and beyond. New technologies will emerge. Contractors will buy new systems and hire new employees. And all the while, internal security teams will be trying to stay a step ahead of hackers and "white hat" security researchers. In short, despite contractors' best efforts, gaps may be identified at any time. Moreover, these gaps may carry with them real consequences — not only the possibility of contract termination, but also the risk of costly and disruptive False Claims Act investigations and lawsuits, with the specter of treble damages, and the possibility of suspension and debarment, lurking. It is thus crucial that contractors continue to be vigilant about the regulations, and take steps to enable them to demonstrate their vigilance and compliance, in order to best position themselves to avoid liability.

The New Requirements

While an in-depth review of the DOD's new cybersecurity requirements is beyond the scope of this short piece, their key elements can be summarized quickly.

The DOD issued the final version of the contract clause set forth at DFARS 252.204-7012 in October 2016.[1] The clause is required in all solicitations and contracts except for those that relate solely to the acquisition of commercial, off-the-shelf items. The clause includes a number of key requirements, including that certain cyber incidents affecting contractors be reported to the DOD,[2] but the most important provision — and the one that has attracted the most attention — directs covered defense contractors to comply with the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," by Dec. 31, 2017.[3] The clause further requires contractors to flow down the NIST SP 800-171 requirements to subcontractors,[4] and a separate provision makes clear that, by submitting an offer in response to a solicitation including the clause, a contractor is representing that "it will implement the security requirements" of NIST SP 800-171 by Dec. 31, 2017.[5] For all contracts awarded prior to Oct. 1, 2017, contractors are further required to notify the DOD chief information officer (CIO) within 30 days of contract award, of any NIST SP 800-171 requirements not implemented at the time of the award.[6] The DOD's CIO is further authorized to adjudicate contractor requests to vary from the NIST requirements, determining whether they are "nonapplicable" or if the contractor has "alternative, but equally effective, security measure[s] in place."[7]

These requirements are not trivial. NIST SP 800-171 details 14 families of controls contractors must implement, and each family contains numerous specific controls, such that the NIST SP 800-171 details well over 100 controls in total. Recognizing this complexity, and the fact that many contractors were scrambling to meet the deadline, the DOD issued guidance in September 2017. This guidance stated that, to "document implementation of the NIST SP 800-171 security requirements by the Dec. 31, 2017, implementation deadline, companies should have a system security plan in place, in addition to any associated plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems."[8] NIST also released draft guidance on

implementing the controls in November 2017, noting that the guidance was “intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements” in NIST SP 800-171.[9]

Continuing Obligations

The intense focus on the Dec. 31 deadline for meeting the new requirements is understandable. The DOD has made clear that cybersecurity is a major focus — indeed, the DOD’s global cyber strategy identifies protecting its own networks, systems and information as one of its three primary missions in cyberspace[10] — and the contracting community justifiably believes the DOD will pay special attention to compliance with the new requirements. Thus, although emerging gaps in cyber risk management programs may present legal, operational, financial and reputational risk in any industry, the risks (as described in more detail below) are particularly acute for contractors, because gaps can place them out of compliance with the DFARS NIST standards. Subsequent invoices for payment under the contracts could present risks of significant liability under the False Claims Act.

That’s why it is particularly important for contractors to realize that compliance with the DFARS requirements is a continuing obligation. A contractor, for all of its best efforts, may have gaps on the Dec. 31 deadline. But even if it does not, the evolving nature of cyber risk and IT environments heightens the potential for a gap to emerge in the future. Consider just a few of the NIST directives: “separate the duties of individuals to reduce the risk of malevolent activity without collusion”; “ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities”; “establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles”; and “track, review, approve or disapprove, and audit changes to organizational systems.”[11] These provisions are in no way unique among the more than 100 NIST requirements in that they either explicitly contemplate that contractors will monitor compliance on an ongoing basis, or make clear that, as systems and workforces change, contractors will need to take steps to ensure their continued compliance. Continued compliance is a challenge, and internal communications and reporting about the compliance status may be a greater challenge still.

Moreover, contractors should be aware that their IT departments and procurement officers are not the only ones looking for compliance shortfalls. Hackers are continually probing and attempting to infiltrate systems and steal information. So too are “white hat” security researchers. And the False Claims Act is not an enforcement tool used only by the government; it incentivizes self-proclaimed “whistleblowers” to search for arguable contract compliance issues and spin them into allegations of fraud on the government, which they then pursue in qui tam lawsuits they file in federal district court, in the name of the government, in the hopes of claiming a bounty in the form of a percentage of any recovery.[12] In short, contractors may learn about security gaps when they least expect it — and with little time before having to report the incident that exposed the gap to the DOD or defend their security publicly.

Dramatic Consequences

As noted briefly above, the potential consequences of compliance gaps only magnify their importance. The DOD’s emphasis on cybersecurity means that, at the very least, such gaps could become a key component of contracting decisions. The DOD will also likely make it a focus of general contractual oversight and contract audits, and compliance problems could lead to contract termination or even suspension and debarment. Contractors recognize these potential contractual consequences as they prepare for the Dec. 31, 2017 compliance date. What is worth emphasizing, however, is that these are not the only potential consequences contractors may face, as the False Claims Act presents an entirely separate category of risks.

Misrepresentations are the bedrock of False Claims Act liability, and over the years both the government and private whistleblowers have sought to expand liability to contractor noncompliances with all manner of the statutory, regulatory and contractual requirements under which contractors operate. Most significantly, the government and whistleblowers have long argued for a theory of implied certification,

according to which a contractor submitting a claim for payment would be deemed to have impliedly certified compliance with all applicable requirements and any noncompliance would render the implied certification false. Last year, in Universal Health Services Inc. v. United States ex rel. Escobar, 136 S. Ct. 1989 (2016), the U.S. Supreme Court recognized this theory but with significant limitations. First, the court held that liability could exist where a contractor made specific representations about the goods or services provided and the contractor's failure to disclose noncompliances with underlying material statutory, regulatory or contractual requirements rendered the affirmative representations misleading.[13] Second, the court made clear that the materiality standard is "demanding," and only those noncompliances with requirements that are material to the government's payment decision are actionable.[14] In this regard, the court also made clear that the government's actual practices regarding a particular requirement are critically important; a requirement may be labeled a condition of payment in a statute or regulation and not be one in practice, and on the other hand a requirement may actually be a condition of payment in practice even if not explicitly labeled as such.[15]

Although the Escobar opinion does not lay out a bright-line test for determining materiality in every case, it is not difficult to imagine courts concluding that at least some cybersecurity compliance shortfalls would be material to the government's payment decision regarding a contract invoice. To be sure, the court explicitly stated that "minor or insubstantial" noncompliances cannot support a finding of materiality.[16] And it also noted, as discussed above, that labels placed on requirements are not necessarily conclusive. But even before the looming DFARS 252.204-7012 implementation date and thus before there is a body of experience regarding the DOD's practical treatment of the requirements, it is clear that the DOD thinks cybersecurity is critically important; indeed, it repeatedly emphasized cybersecurity risks and refused to grant an extension of the DFARS cybersecurity requirements. It's thus not hard to imagine scenarios where noncompliance with the NIST SP 180-171 requirements would raise at least a serious question of materiality.

Steps to Take

Given the importance of the DOD's new cybersecurity requirements, and the potential consequences of noncompliance, contractors must take steps to protect themselves. Here are three we would recommend:

1. Put in place appropriate continuous monitoring and assessment programs — both internal and third-party.

Cybersecurity is never a "one-and-done" task. Even the most robust cyber risk management programs require a feedback loop to ensure that policies and procedures are implemented, and that human error, changing technologies or new business practices have not introduced a vulnerability. Continuous monitoring and auditing also provides valuable record-keeping about your good faith compliance efforts, which could become an important part of establishing that you lacked the requisite scienter for certain types of liability if a gap is later discovered.

In addition to internal monitoring and auditing processes, most mature cybersecurity programs will also have occasional, if not quite regular, third-party audits or assessments. Such audits place a fresh set of eyes on a contractor's program, and enable companies to both establish a record of compliance and independently document the steps they have taken to close gaps identified in prior audits by the next audit period.

In certain high-leverage circumstances, moreover, it may be appropriate to have outside counsel lead a third-party assessment. Outside counsel can bring in appropriate security vendors to conduct an assessment; ensure that the results of the assessment and a contractor's general security practices are documented appropriately, with an eye toward possible future legal risks; and provide privileged legal advice on the results of the assessment with regard to its cyber risks — including, as described in more detail below, potential False Claims Act exposure.

2. Respond appropriately to the unexpected discovery of cyber vulnerabilities by conducting a forensic investigation.

As noted earlier, companies can discover cyber vulnerabilities in many ways: hackers can exploit them, white hat researchers can publicize them, and whistleblowing insiders can identify them. Moreover, hindsight is almost always 20/20 — particularly when a cybersecurity program is subjected to scrutiny in the wake of an incident — and vulnerabilities may thus create real risks, including with respect to the False Claims Act. It is therefore important for covered contractors to conduct a forensic investigation at the direction of counsel and under privilege immediately after discovering a vulnerability.

A forensic investigation directed by counsel helps a contractor investigate the source, scope and circumstances of the breach, as well as identify and fulfill its legal obligations with regard to that breach. Such an investigation further allows the contractor to evaluate its compliance status at the time of the incident and position the company most effectively to meet the DFARS clause's requirement that cyber incidents be investigated and reported to the DOD within 72 hours. An investigation will also help the company understand any risks it may face under the False Claims Act and other laws with regard to the incident. This would include whether the circumstances additionally trigger FAR clause 52.203-13's mandatory disclosure requirements concerning credible evidence of False Claims Act and other violations or whether, as discussed below, it would be prudent even in the absence of such a trigger to self-report concerns to contracting officials to help mitigate possible False Claims Act risk. Indeed, in certain circumstances, self-reporting is most effective before an incident starts to gain publicity or the government begins to investigate of its own accord. Thus, companies should consider putting in place plans governing how they are going to react, begin their privileged investigation, and make critical decisions in a timely fashion.

3. Remediate gaps identified in audits or by breaches immediately and, consulting with counsel as necessary, take appropriate next steps.

When audits or assessments identify compliance gaps, or gaps are exposed by breaches, it is important for companies to address these gaps quickly. Certain legal risks turn on a contractors' knowledge of vulnerabilities — for example, liability under the False Claims Act generally turns on whether the defendant acted "knowingly."[17] It is thus vital for contractors to close gaps expeditiously.

Moreover, in addition to expeditiously developing remediation plans, contractors should consider informing their contracting officer or other appropriate official of their findings, even in the absence of circumstances calling for a mandatory disclosure. In Escobar, the Supreme Court made clear that, "if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material" for False Claims Act purposes.[18] Timely informing the Government of identified vulnerabilities can thus potentially help to mitigate future False Claims Act risks.

Colleen Brown, Robert J. Conlan and Christopher C. Fonzone are partners in the Washington, D.C. office of Sidley Austin LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See 81 Fed. Reg. 73000.

[2] See 48 C.F.R. 252.204-7012(c).

[3] See id. at (b)(2)(i).

[4] See id. at (m).

[5] See 48 C.F.R. 252.204-7008.

[6] See 48 C.F.R. 252.204-7012(b)(2)(ii)(A).

[7] See id. at (b)(2)(ii)(B).

[8] Memorandum from Shay D. Assad, Re: Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, at 3 (Sept. 21, 2017).

[9] Draft NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information, at iv (November 2017)

[10] The Department of Defense, The DOD Cyber Strategy, at 4-6 (April 2015).

[11] NIST Special Publication 800-171, Protecting Unclassified Information in Nonfederal Information Systems and Organizations, at 9-10 (June 2015).

[12] See 31 U.S.C. § 3730.

[13] Escobar, 136 S. Ct. at 2001.

[14] Id. at 2002-03.

[15] Id. at 2003-04.

[16] Id. at 2003.

[17] See 31 U.S.C. § 3729(a)(1).

[18] Escobar, 136 S. Ct. at 2003.

Article Link: https://www.law360.com/cybersecurity-privacy/articles/994933/dfars-cyber-compliance-and-potential-for-fca-risk