Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity Enforcement Shouldn't Be Left To FCA Relators

By **Robert Metzger and Stephen Bacon** (May 16, 2019, 5:28 PM EDT)

Robert Metzger

Stephen Bacon

In recent years, the U.S. Department of Defense and other federal agencies, including NASA, have issued acquisition regulations that impose new cybersecurity requirements on contractors.[1] These measures have taken on increasing urgency as reports continue that foreign nation state adversaries continue to use cyber means to gain unauthorized access to and then "exfiltrate" — steal — intellectual property and other sensitive, unclassified information from defense and space contractors.

On May 8, 2019, a the U.S. District Court for the Eastern District of California issued what appears to be the first decision to address the intersection between cybersecurity requirements and the False Claims Act.[2] In Markus v. Aerojet Rocketdyne Holdings Inc., the court held that a qui tam plaintiff alleged sufficient facts to satisfy the FCA's "materiality" standard based on claims that the contractor misrepresented its compliance with cybersecurity requirements to fraudulently obtain contracts with the DOD and NASA.

This decision presents some demanding and urgent questions. Few would disagree that contractors must improve their cyber defenses to staunch the loss of critical data to adversaries. And many would agree that present federal contract methods have failed to improve security for much of the defense and space industrial base. The absence of accountability and minimal risk of noncompliance have contributed to the problem. The Markus decision undoubtedly will sound the alarm to many in industry.

Regulatory Background

The DOD's efforts to protect sensitive information on contractor networks has a long and complicated history which is beyond the scope of this article. To appreciate the implications of Markus, however, a basic understanding of the DOD's cybersecurity regulatory regime is helpful.

In 2013, the DOD issued a final rule that required contractors to protect unclassified controlled technical information, or CTI, using some cyber safeguards derived from the National Institute of Standards and Technology, or NIST, special publication 800–53.[3] Because the safeguards imposed by SP 800-53 generally apply to federal information systems, security requirements in SP 800-53 were not necessarily

intended for use protecting information systems owned and operated by contractors.

In June 2015, NIST issued SP 800-171 with safeguards specifically tailored for use in protecting contractor information systems. On Aug. 26, 2015, the DOD issued an interim rule[4] that abandoned the CTI definition used in the prior final rule.

The DOD expanded the scope of protected material to include covered defense information, or CDI. CDI encompassed CTI — which has military or space significance — as well as all other forms of controlled unclassified information, or CUI, which must be kept confidential by operation of federal law, regulation or government-wide policy.

Under the interim rule, contractors were required to provide "adequate security" for CDI by implementing security controls in SP 800-171 or "[a]lternative but equally effective security measures." Implementation of "alternative measures" required approval "in writing by an authorized representative of the DOD CIO prior to contract award."

In response to criticism from industry, the DOD published a second interim rule[5] on Dec. 30, 2015, which allowed contractors until Dec. 31, 2017, to implement the security requirements specified in SP 800-171. Contractors were required to report on any gaps against SP 800-171 safeguards within 30 days of receipt of a contact subject to DFARS Clause 252.204-7012.

On Oct. 21, 2016, the DOD issued the final network penetration DFARS rule which remains in effect today.[6] The final rule permits contractors to propose variances from any of the security requirements of SP 800-171.

The applicable clause states:

> The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.[7]

The final rule emphasizes that "DFARS Clause 252.204-7012 is not structured to facilitate the use of the contractor's compliance with NIST SP 800-171 as a factor in the evaluation/source selection process."[8]

The director of defense pricing and defense procurement and acquisition policy, or DPAP, issued a guidance memorandum[9] on Sept. 21, 2017, on implementation of the DFARS -7012 clause.[10] This guidance — not cited in the Markus decision — states that contractors are to "self-attest to meeting" the DFARS requirements.

Markus v. Aerojet Rocketdyne

This was not a final decision on the merits. Rather, the court was ruling on a Rule 12(b)(6) motion which, in part, sought to dismiss the FCA allegations in the complaint. To decide a 12(b)(6) motion, the court must accept the allegations of the complaint as true and draw all reasonable inferences in the plaintiff's favor.[11] Accordingly, the court's decision is far from the "last word" even on the allegations of this complaint.

Nonetheless, this decision stands for the proposition that a whistleblower can bring a federal FCA case, alleging a contractor knowingly failed to fulfill contractual cyber requirements, and survive a motion to

dismiss, even where the United States — through the U.S. Department of Justice — investigated the allegations and declined to intervene. That alone warns federal contractors that they face exposure to FCA actions. Cyber defenses and adoption of SP 800-171 safeguards now must be managed with this legal and liability threat in mind.

In 2014, the relator Brian Markus was hired as the senior director of cybersecurity, compliance and controls for Aerojet Rocketdyne Holdings Inc. and Aerojet Rocketdyne Inc., a major aerospace and defense contractor. Aerojet sells rocket engines and other products to the DOD, NASA and prime contractors who perform work for those agencies. The relator alleges he was hired to improve Aerojet's cybersecurity.

The relator claims an outside consulting firm audited Aerojet's compliance with the DOD and NASA[12] cybersecurity requirements in early 2014 and found the company to be "less than 25% compliant." The relator alleges Aerojet entered into at least six DOD contracts and nine contracts with NASA between February 2014 and April 2016. According to the relator, Aerojet misrepresented its compliance with cybersecurity requirements in its communications with government officials relating to the award of these contracts.

The relator claims the DOD and NASA were fraudulently induced into awarding contracts to Aerojet based upon these false and misleading statements. The relator asserts he refused to sign documents in July 2015 indicating that Aerojet was in compliance with cybersecurity requirements. Aerojet terminated the relator's employment on Sept. 14, 2015.

On Oct. 29, 2015, the relator filed a qui tam lawsuit against Aerojet. The relator alleges fraud claims against Aerojet under the FCA based on promissory fraud (i.e. fraud in the inducement) and the submission of fraudulent statements or records. The relator also claims he was wrongfully terminated in retaliation for his internal complaints and refusal to certify Aerojet's compliance with cybersecurity requirements. The United States filed a notice of election to decline intervention on June 5, 2018.

After the complaint was unsealed, Aerojet filed a motion to dismiss on Feb. 22, 2019. Aerojet argued that the relator's complaint failed to allege sufficient facts to satisfy the element of "materiality" under the FCA. A false or misleading statement is material under the FCA if it has "a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property."[13]

In Universal Health Services Inc. v. Escobar, the U.S. Supreme Court described the materiality standard as "demanding" and explained that the FCA is not "a vehicle for punishing garden-variety breaches of contract or regulatory violations."[14] A noncompliance that is "minor or insubstantial" is not material.[15] Whether a particular noncompliance is "material" depends on "the government's conduct in similar circumstances and whether the government has knowledge of the alleged noncompliance."[16]

The court rejected Aerojet's argument that the relator failed to adequately plead materiality on four separate grounds. First, Aerojet argued that the relator could not allege materiality because Aerojet disclosed its noncompliance to the government. Although Aerojet disclosed to the government that it was noncompliant with some cybersecurity requirements, the court held that the relator properly alleged materiality because he claimed Aerojet "did not fully disclose the extent of [its] noncompliance with relevant regulations."[17] The court emphasized that although Aerojet "disclosed some of its noncompliance" it could still be liable for an incomplete or otherwise misleading disclosure.[18]

Second, Aerojet argued that the materiality standard could not be met because the DOD and NASA continued to contract with Aerojet after investigating the allegations in the relator's compliant. The court recognized that "[s]uch evidence is not entirely dispositive on a motion to dismiss" because the materiality inquiry focuses on whether the "alleged misrepresentations were material at the time the government entered into or made payments on the relevant contracts."[19] Because Aerojet's compliance with cybersecurity requirements may have evolved since the award of the contracts at issue, the court was unwilling to consider Aerojet's post-complaint contracts with the DOD and NASA as evidence of materiality at the motion to dismiss stage. The court also held that the government's decision not to intervene in the case was not a factor relevant to materiality.[20]

Third, Aerojet maintained that the alleged misrepresentations were not material because they did not go to the "essence of the bargain." The court found this argument unavailing. Although Aerojet's contracts with the DOD and NASA did not relate specifically to cybersecurity, the relevant acquisition regulations and contract clauses require contractors to satisfy specific requirements to handle sensitive technical information. In the court's view, Aerojet's alleged noncompliance with these requirements may have hindered its ability to handle sensitive information during performance of the contract.

Finally, Aerojet argued that materiality was lacking because recent DOD regulatory history provides strong evidence that the government did not expect full "technical compliance" with all security measures. Aerojet observed that the DOD amended the clause to "relax" the applicable requirements from SP 800-53 to SP 800-171 and then extended the "full compliance" deadline for DFARS Clause 252.204-7012 until Dec. 31, 2017. Aerojet further argued that Revision 1 of SP 800-171, published in December 2016, allowed contractors to achieve "compliance" with the "adequate security" requirement so long as they prepared system security plans, or SSPs, and plans of action and milestones, or POAMs, to document the steps they will take in the future to comply with all security controls. The court found that Aerojet's observations were not dispositive because the relator properly alleged "that the extent to which a company was technically compliant still mattered to the government's decision to enter into a contract."[21]

Aerojet's motion to dismiss was denied as to the relator's principal fraud claims.[22] The relator's employment-based claims were referred to arbitration.

Analysis

Exposure to qui tam suits and potential fraud liability will motivate companies to act. The Markus decision signals to defense and space contractors that they now face that exposure for their cybersecurity measures. While some may consider this to be a salutary effect, the FCA is the wrong tool to address a problem that is at once serious, urgent and complex. Contractor cybersecurity should not become another feeding ground for the qui tam plaintiff's bar.

In the Markus ruling, the court accepted, as true, that "how close [Aerojet] was to full compliance was a factor in the government's decision to enter into some contracts."[23] This suggests a standard of liability for cyber noncompliance with little foundation in existing law, regulation or policy. The notion that companies face FCA exposure absent complete satisfaction of every cyber requirement cannot be reconciled with the actual technical and operational challenges of securing contractor information systems. Threats are constantly evolving and cybersecurity solutions necessarily vary among contractors to reflect individual means and circumstances.[24] Expectations of "perfect" security are commendable only in theory, but unachievable in practice.

The court's approach to the critical "materiality" inquiry suggests that companies may be forced to litigate, over years and at vast expense, whether or not a given government customer would have awarded a contract had it known that the company's cybersecurity was imperfect at the time of offer and award. This is not how the federal government should act to gain assurance of contractor cybersecurity.

The government has many ways to administer and enforce cyber requirements. Cyber compliance can be a matter of "contractor responsibility" such that validated security operates as a condition of eligibility for certain contracts. In solicitations, the government can require disclosure of SSPs and POAMs and these can be evaluated for adequacy or scored as competitive discriminators. A company's relative level of cyber assurance can be independently evaluated. Companies already are subject to DCMA cyber review and other methods, such as system monitoring, can be selectively required to validate security. All of these are now in the works or under study by the DOD or the military services.

The FCA is not necessary to enforce contractor cyber compliance. It is for a federal requiring activity, or contracting officer or oversight official to decide what level of risk they are willing to accept as companies work towards full compliance with DFARS and NIST cyber requirements. The government should rely not upon the FCA but upon methods that are risk-informed, reflect real consequences — rather than presumed injury — and which can be tailored to customer requirements, program-specific risk tolerance and contractor circumstances.

The Markus decision could have another dysfunctional consequence. It might cause companies to avoid meaningful but potentially "negative" conclusions in either SSPs or POAMs — lest such documents, in the hands of a relator's counsel, become prima facie evidence of less than "full compliance." This would defeat the purpose of preparing SSPs and POAMs. SSPs and POAMs, by definition, are intended to inform companies of the present status of their security, identify shortcomings and present objectives for improvement. The government should encourage, not penalize, companies to prepare fulsome SSPs and POAMs.

Ultimately, government and industry should work together, not as adversaries, to respond to a common threat. Federal courts should be reluctant to assume the responsibility to "adjudicate" the adequacy of contractor cyber measures.

There will be instances where companies promise security to a federal customer that they do not deliver. There can be situations, as was alleged in Markus, where a company knowingly or recklessly misleads the government. The government should deter such conduct and, when necessary, punish it.

Enforcement should be the exclusive responsibility of the government. If a government customer has cause for objection regarding cyber compliance, it can exclude that company from further award, demand improvements during contract performance, potentially terminate a contract for default and seek damages should injury occur. It can even seek to disbar a contractor. In extreme cases, the government can bring civil or criminal actions for false claims or fraud. However, the False Claims Act should be amended, or construed, to remove cybersecurity as a compliance domain that can be exploited by private "whistleblowers". The risk of indiscriminate outcomes and broad damage to the companies in the supply chain is too great, the likelihood of public benefit too small.

As shown by Markus, FCA law today has room for a plaintiff to exploit "bad facts" — such as those in the Markus pleading — to produce FCA exposure. Congress may need to act to narrow the use of the FCA in cases involving cyber compliance. Until then, however, at the very least companies should take from

Markus the necessity of respecting and responding to dissenting views of internal employees who have cyber expertise and responsibility. Suppressing such views, while acting in ways that seem intended to mislead the government customer, will render companies at risk of drawn-out, costly-to-defend qui tam lawsuits.

Robert S. Metzger is a shareholder at Rogers Joseph O'Donnell PC and a co-author of the August 2018 MITRE Corporation Deliver Uncompromised report.

Stephen L. Bacon is an associate at the firm.

[1] See DFARS Clause 252.704-7012; NASA FARS Clause 1852.204-76.

[2] U.S. ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc. https://www.govinfo.gov/content/pkg/USCOURTS-caed-2_15-cv-02245/pdf/USCOURTS-caed-2_15-cv-02245-5.pdf

[3] 78 Fed. Reg. 69273 (Nov. 18, 2013).

[4] 80 Fed. Reg. 51739 (Aug. 26, 2015).

[5] 80 Fed. Reg. 81472 (Dec. 30, 2015).

[6] 81 Fed. Reg. 72986 (Oct. 21, 2016).

[7] DFARS Clause 252.204-7012(b)(2)(ii)(B).

[8] 81 Fed. Reg. 72986, 72990.

[9] https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf

[10] DPAP Memorandum, Sept. 21, 2017, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," available at https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[11] Accordingly, in this decision the court did not rule that any of the allegations in the complaint, regarding the security practices of the defendant, or otherwise, were true. As the case proceeds, defendants may be able to succeed with any number of potential defenses.

[12] The applicable NASA FARS Clause requires contractors to protect "Sensitive But Unclassified" (SBU) information from unauthorized disclosure. NASA FARS Clause 1852.204-76(b). The Clause does not require implementation of SP 800-171, but refers to "[a]pplicable requirements, regulations, policies, and guidelines" identified on an applicable documents list attached to the contract.

[13] 31 U.S.C. §3729(b)(4).

[14] Universal Health Services Inc. v. U.S. et al. ex rel. Escobar et al.,136 S. Ct. 1989, 2003 (2016).

[15] Id.

[16] Opinion at 7 (citing Escobar at 136 S. Ct. at 2003).

[17] Opinion at 8 (emphasis added).

[18] Opinion at 9 (emphasis in original).

[19] Opinion at 11.

[20] Opinion at 12.

[21] Opinion at 13.

[22] The court granted Aerojet's motion to dismiss the relator's conspiracy claims under the FCA. Under the "intracorporate conspiracy doctrine," a parent corporation cannot conspire with its wholly-owned subsidiary. Moreover, a corporation cannot conspire with its own employees or agents. The court dismissed the relator's conspiracy claim because he failed to allege that Aerojet conspired with any independent individual or entity.

[23] Opinion at 10.

[24] The DPAP guidance memorandum also says that "[t]here is no single or prescribed manner in which a contractor may choose to implement the requirements of NIST SP 800-171, or to assess their own compliance with those requirements." It further states that "[u]ltimately, it is the contractor's responsibility to determine whether it has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information."