A FAILURE TO IMPLEMENT CYBERSECURITY MEASURES COULD LEAD TO FALSE CLAIMS ACT LIABILITY FOR DEFENSE CONTRACTORS

Date: 26 January 2018

U.S. Federal, State and Local False Claims Act Alert

By: Samuel P. Reger, Matthew R. Hubbell, Stuart B. Nibley

Add another item to the list of ways a defense contractor could face False Claims Act ("FCA") liability: material noncompliance with cybersecurity regulations. Although this theory of liability has not yet been tested in courts, it appears ripe for litigation.

On the cybersecurity side:

1. The Department of Defense ("DOD") now requires contractors with covered defense information to have adequate cybersecurity controls in place ("DOD Cybersecurity Controls"). [1]
2. On May 11, 2017, President Trump mandated that all U.S. federal government agencies adopt cybersecurity measures developed by the National Institute of Standards and Technology ("NIST"). [2]
3. There is increased awareness that state-sponsored entities and "hacktivist" groups are targeting confidential information of the government and others (e.g., "Shadow Brokers" reportedly obtaining highly classified National Security Agency information; reported hacking attempts by China, South Korea, and Germany into Hilary Clinton's private e-mail server; and North Korea allegedly being directly responsible for the "WannaCry" ransomware attack).

On the FCA side, the Supreme Court has confirmed that implied certification claims can be brought against contractors based on material noncompliance with legal or contractual requirements. [3]

MATERIAL NONCOMPLIANCE WITH CYBERSECURITY REQUIREMENTS COULD LEAD TO FCA LIABILITY.

The FCA imposes draconian treble damages and penalties for those who defraud the government by knowingly making a material false claim or statement. [4] It is most simply applied in situations where a government contractor either overbills for completed work or bills for work that was never completed.

However, in *Escobar*, the Supreme Court said that FCA "liability can attach when the defendant submits a claim for payment that makes specific representations about the goods or services provided, but knowingly fails to disclose the defendant's noncompliance with a statutory, regulatory, or contractual requirement." [5] Importantly, though, because the FCA is not meant to turn garden-variety contract claims into fraud, the analysis focuses on whether the noncompliance was "material" to the payment. [6] "What matters is not the label that the Government attaches to a requirement, but whether the defendant knowingly violated a requirement that the defendant knows

is material to the Government's payment decision." [7] Thus, under *Escobar*, only material noncompliance can lead to FCA liability.

MATERIALITY UNDER *ESCOBAR*.

Under the FCA and common law, materiality "look[s] to the effect on the likely or actual behavior of the recipient of the alleged misrepresentation." [8] Various factors affect whether noncompliance is material:

4. A contractor expressly certifying compliance makes a finding of materiality more likely. [9]
5. The government requiring compliance as a condition of payment makes a finding of materiality more likely. [10]
6. A record of the government regularly refusing to pay claims based on a particular type of noncompliance makes a finding of materiality more likely. [11]
7. A record that the government regularly pays a particular type of claim in full despite actual knowledge that certain requirements were violated, and has signaled no change in position, makes a finding of materiality less likely. [12]
8. A record that the government paid a particular claim in full despite its actual knowledge that certain requirements were violated makes a finding of materiality less likely. [13]
9. Noncompliance that goes "to the very essence of the bargain" between the government and the contractor makes a finding of materiality more likely. [14]

Because no one factor above is determinative, the balance of the factors must overcome, as the Supreme Court put it, the "demanding" materiality standard. [15]

VIOLATION OF REGULATIONS REQUIRING CYBERSECURITY MEASURES MIGHT SUPPORT A FINDING OF MATERIALITY UNDER THE FCA.

In a 2016 case, which hits close to the subject matter of this article, a court examined whether noncompliance with the Health Information Technology and Clinical Health Act ("HITECH Act") could lead to FCA liability for a health care provider. [16] Under the HITECH Act, health care providers receive incentive payments to implement cybersecurity measures. In *Kettering*, a relator argued that her health care provider failed to implement the cybersecurity measures, and, to support her claim, she alleged that her own protected health information had been compromised. [17] The court ultimately dismissed the FCA claim, recognizing that a security breach is not de facto evidence of inadequate security measures. Instead, the court said that the relator had to allege facts to support her allegation that the health care provider had not implemented the requisite policies and procedures. [18] Notably, the court dismissed the case on the basis of a failure to plead adequate facts, perhaps suggesting that, if adequate facts had been pleaded, a failure to implement required cybersecurity measures could lead to a FCA violation. [19]

THE DOD CYBERSECURITY CONTROLS WILL LIKELY LEAD TO INCREASED FCA RISK FOR DEFENSE CONTRACTORS.

Projecting forward from this caselaw, contractors with sensitive information could be especially vulnerable under current regulations. The DOD Cybersecurity Controls are actually styled as a contract clause that must be inserted into every contract with the DOD, except those related to basic commercial items. [20] The practical effect of this clause is that most defense contractors will now expressly certify that they have implemented the prescribed cybersecurity controls, which by itself makes a materiality finding more likely. [21]

Under the DOD Cybersecurity Controls, contractors with covered defense information are required to provide "adequate security" (generally, compliance with National Institute of Standards and Technology Special Publication (SP) 800-171) and to report cyber incidents within 72 hours (an extremely short period of time compared to other reporting laws, which generally provide at least 30 days). [22] Covered contractors are also required to make sure their subcontractors comply with the controls. [23] This type of specific regulation aimed at contractors who obtain defense information would likely be a factor that weighs in favor of materiality.

Regardless, contractors should take cybersecurity certifications seriously, even if it is just for business purposes. The White House, in May 2017, required federal agencies to adopt a previously voluntary framework of cybersecurity standards developed by NIST. [24] The executive order makes agency heads directly accountable to the president for managing the cybersecurity risk that their agencies face. [25] This additional pressure will likely flow down, in the form of certifications, audits, or other oversight, to those that contract with government agencies. Noncompliance could result in suspension or affect a contractor's ability to receive future contracts.

CONSIDERATIONS FOR DEFENSE CONTRACTORS WITH CYBERSECURITY OBLIGATIONS

Defense contractors, in light of recent regulations and an increased emphasis on cybersecurity by federal agencies, will likely be required to make an express certification that they have adequate cybersecurity measures in place. Moreover, whistleblowers may pursue FCA claims under an implied certification theory premised on alleged noncompliance with those cybersecurity requirements. At the threshold, contractors should determine whether a failure to implement cybersecurity measures would influence payment from the government, i.e., whether such failure would be material. Defense contractors should also consider involving counsel when building a cybersecurity program. Cyber threats facing defense contractors and the laws regarding cybersecurity can be complex. It is common for companies to find that state, federal, and international cybersecurity laws apply. Further, because cybersecurity laws or standards are usually not prescriptive, the requirements for the program will change over time based on the risks that the defense contractor faces. Counsel can assist in developing an effective, risk-based program that addresses applicable laws and mitigates the risk of FCA enforcement.

---

[1] 48 C.F.R. § 252.204-7012.

[2] Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Reg. 22,391 (May 11, 2017).

[3] *Universal Health Servs. Inc. v. United States et al. ex rel. Escobar*, 136 S. Ct. 1989 (2016) (cited as "*Escobar*").

[4] 31 U.S.C. § 3729(a)(1)(G).

[5] *Id*. at 1995.

[6] *Id*. at 2003.

[7] *Id*. at 1996.

[8] *Id*. at 2002.

[9] See *Escobar*, 136 S. Ct. at 2001. *United States ex rel. Se. Carpenters Reg'l Council v. Fulton Cty., Ga*., 2016 WL 4158392, at *5 (N.D. Ga. Aug. 5, 2016) ("The misrepresentation, whether express or implied, 'must be material to the other party's course of action.'") (quoting *Escobar*, 136 S.Ct. at 2001).

[10] *See United States ex rel. Kelly v. Serco, Inc.,* 846 F.3d 325, 334 (9th Cir. 2017) (holding that the noncompliance was immaterial because it was related a "minor contractual provision" and "ancillary" to the contract's purpose).

[11] *United States v. Sanford-Brown, Ltd.,* 840 F.3d 445, 447 (7th Cir. 2016) (failing to establish materiality because no evidence that the government's "likely or actual behavior" would have been different had it known of the noncompliance).

[12] See *Escobar*, 136 S. Ct. at 2003–04.

[13] *Id*.

[14] *United States ex rel. Escobar v. Universal Health Servs., Inc*., 842 F.3d 103, 110 (1st Cir. 2016).

[15] See *Escobar*, 136 S.Ct. at 2003.

[16] *United States ex rel. Sheldon v. Kettering Health Network*, 816 F.3d 399 (6th Cir. 2016).

[17] *Id*. at 409–10.

[18] *Id*. at 411–12.

[19] *Id*. at 414.

[20] § 204.7304(c).

[21] See *Escobar*, 136 S. Ct. at 2001 ("[W]hen evaluating materiality under the False Claims Act, the Government's decision to expressly identify a provision as a condition of payment is relevant. . . .")

[22] § 252.204-7012(m).

[23] § 252.204-7012.

[24] 82 Fed. Reg. 22,391.

[25] *See id.*

