October 22, 2018 - Cybersecurity & Data Privacy, Defense

GUIDANCE ON SECURING CONTROLLED UNCLASSIFIED INFORMATION – KEY TAKEAWAYS FROM THE NIST CUI WORKSHOP

By: Tina Reynolds

On October 18, 2018, the National Institutes for Standards and Technology (NIST) hosted a day-long workshop that featured experts from across the government brought in to educate industry representatives and government agency personnel about the security requirements applicable to Controlled Unclassified Information (CUI). Hundreds of attendees, both in person and via webcast, turned out to learn more about the implementation and assessment of CUI security requirements.

Important new information about future regulations and publications was revealed at the conference, and agency positions about the operation of current rules were discussed. Several of the most significant highlights follow.

1. **Government and Industry Are "One Team, One Mission."**

A theme of the conference, and the title of Dr. Ron Ross's opening keynote, this phrase emphasizes the critical role industry plays in protecting sensitive government information and data. All speakers acknowledged that both government and industry are vulnerable to cyber threats. We have tools to address known vulnerabilities, but need to move beyond this first stage to a point where we can prevent and detect "zero day" vulnerabilities, which may launch in the future, and anticipate advanced persistent threats, which may be capable of taking down (or taking control of) entire systems. Conceptually, not only should companies be hardening targets with basic system security, but they should attempt to limit damage to the target if compromised through measures such as domain separation, network segmentation, and virtualization.

2. **The FAR CUI Clause Will Debut in 2019.**

The highly anticipated FAR CUI clause will give agencies a mechanism to extend the National Archives and Records Administration (NARA) CUI rules to contractors. (They currently apply only to government agencies). The drafters of the FAR clause noted that they are taking pains to address what they know are significant contractor concerns about how to identify what is CUI that requires protection. As currently envisioned, the FAR clause will put the burden on the contracting agency, as part of the contracting process, to identify all CUI expected to arise in the course of performance. This would include not only CUI to be provided by the government, but also CUI to be generated by the contractor.

The FAR CUI clause is expected to differ from the current DFARS 252.204-7012 clause in a few key ways. First, although the -7012 clause refers to CUI as part of the definition of "covered defense information" (CDI), the DFARS clause does not implement the NARA CUI program in full. For example, it does not address marking requirements. The FAR clause will be more expansive. Second, the DFARS clause requires contractors to identify which of their contractor-generated information is CDI, while, as mentioned above, the FAR clause will put this burden on the government. DoD representatives at the conference noted that upon publication of the FAR clause the DFARS clause will be revised to address duplicative language and conflicts with the FAR clause, although some portions of the DFARS clause not addressed by the new FAR rule may remain, such as the DIBNet reporting process for cybersecurity incidents.

The FAR CUI clause will be consistent with the DFARS in that it will rely on NIST 800-171 as the framework for security requirements.

Before becoming final, a draft rule will go out to agencies and the public for comment. NIST and NARA representatives at the conference strongly encouraged contractors to provide constructive commentary on the draft rule.

3. **A Forthcoming Revision to NIST SP 800-171 Will Add New, "Optional" Requirements.**

Revision 2 to the NIST SP 800-171 is likely to be published in March 2019. The revision will describe more extensive requirements that might be implemented by contractors handling critical defense and infrastructure information – information which, if compromised, could lead to significant damage. Whereas the current 800-171 requirements are designed to establish "adequate security," the new requirements would add a layer of protection specifically designed to address advanced persistent threats. Where appropriate, agencies

could mandate compliance with the Rev. 2 "optional" requirements. Even where not mandated, contractors might choose to implement the new requirements as an added element of security.

4. **"Soon" Someone Within the Government Will Be Given Responsibility for Assessing Contractor Cybersecurity Compliance.**

In most instances, contractors are asked to self-certify compliance with the DFARS -7012 clause and 800-171. Increasingly, however, cybersecurity is becoming a factor in proposal evaluation, leading to program-level reviews of security controls. Some contracts contain provisions for post-award audits or self-reporting of cybersecurity of compliance. In addition, the DoD Inspector General has undertaken targeted compliance audits, and the Defense Contract Management Agency (DCMA) has been given some cybersecurity compliance oversight responsibility. This diffuse and somewhat duplicative authority has been a source of confusion and frustration for contractors. Once the FAR CUI clause is in effect, there will be even more possible assessors of compliance within government.

DoD and NIST personnel recognized this problem, and indicated that efforts are being made to address the situation. They indicated that "soon" it is anticipated there will be one "government-wide" assessor of compliance.

Multiple contractors also asked why the DFARS and NIST 800-171 do not have a requirement for third-party assessment, as is the case with FedRAMP. The government panelists universally indicated that they did not think such a requirement was feasible or appropriate for use in determining NIST 800-171 compliance. First, the government did not want to create a "cottage industry" of assessors. So many would be needed that there could not be a rigorous certification process, as there is for third-party assessment organizations under FedRAMP. Results of third-party assessment would therefore be unreliable and inconsistent. In addition, in the event of a problem, it would not be clear whether the assessor or the contractor would be to blame.

The speakers noted that the new FAR CUI clause will not have a third-party assessment component. The idea is being considered within government, however, as relates to very high-risk situations.

5. **Many Contractors Have the Same Questions About CUI and the DFARS Cybersecurity Rule.**

In addition to confusion about what qualifies as CUI, several common questions and areas of frequent misunderstanding were identified at the conference.

A. How Do Security Controls Apply to the Cloud?

Several contractors asked questions about when NIST 800-171 security controls must be met in a cloud environment where the DFARS -7012 clause applies. The basic rules can be summarized as follows:

- If the contractor is operating its own cloud, it must follow NIST 800-171.
- If the contractor is using a third-party cloud service provider (CSP), the CSP, per DFARS 252.204-7012(b)(ii)(D), must be able to meet the FedRAMP Moderate baseline. (DoD representatives made the point that the CSP does not have to be FedRAMP *certified*, it only must be able to demonstrate that it meets the FedRAMP Moderate requirements.) The CSP does not have to comply with the rest of the DFARS clause, but it must allow the contractor to meet its cyber incident reporting obligations in 252.204-7012(c)-(h). The agreement between the contractor and CSP should capture this requirement.
- If the contractor is operating a cloud-based system on behalf of the government, then DFARS 252.239-7010 applies instead of the -7012 clause. The contractor must meet the DoD System Requirement Guidelines and all other requirements for government systems.

B. What Happens After a Company Reports a Cybersecurity Incident Via DIBNet?

After a report is made to DIBNet, the DoD cybercrime center (DC3) makes a decision whether or not the information is critical enough that DoD needs more information, which it can request and collect pursuant to 252.204-7012(d)-(g). In its initial assessment DC3 looks at the information compromised and how it could impact weapons systems or defeat defensive military capabilities. DC3 also analyses the report to identify cyber threat vectors and adversary trends.

It is important to note that per DFARS 204.7302(d), the mere fact that a cyber incident has occurred and been reported is not, in and of itself, evidence of inadequate security.

C. What About Supply Chain Risk?

Another point that was not lost on either the speakers or the audience was that hardware, firmware, and circuits may contain embedded vulnerabilities that the DFARS -7012 clause and NIST 800-171 do not address. These are supply chain issues that are being considered in conjunction with the forthcoming Risk Management Framework 2.0.

D. What Help Is Available for Contractors Working on 800-171 Compliance?

Government speakers emphasized the many readily available, and free, resources to help contractors assess and come into compliance with NIST 800-171. NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," for example, contains specific guidelines for assessment. The Department of Homeland Security also has assembled a Cybersecurity Evaluation Tool (CSET), which has a module for NIST 800-171. In addition, Procurement Technical Assistance Programs have been set up to help small businesses in particular.

The speakers urged that contractors be wary and do their homework when hiring consultants. They observed that some consultants identify problems and then try to sell their products as solutions when other, less costly solutions might have been available. The general view was that contractor IT personnel know their systems better than anyone else, and are therefore typically in the best position to assess compliance, so long as they are honest with themselves in identifying areas that could be improved.

Additional information about the NIST workshop is available here. To see the day's slide presentations, expand the "Agenda" item.

May 15, 2019 - Cybersecurity & Data Privacy, Defense, False Claims Act

FEDERAL COURT CONFIRMS THAT CYBERSECURITY GAPS CAN FORM THE BASIS OF FALSE CLAIMS ACT VIOLATIONS

By: Alex Ward, Tina Reynolds and David Allman*

Since the Department of Defense (DoD) and other federal agencies began implementing formal cybersecurity requirements for government contractors within the last few years, one lingering question on the minds of federal contractors and subcontractors has been: "What happens if I do not comply?" Firms, including ours, have counseled that breach of contract claims are possible, and cautioned against misrepresentations of compliance. Now a federal district court has confirmed what has long been suspected, that failure to abide by contractual and regulatory cybersecurity requirements may lead to liability under the False Claims Act.

In *United States of America ex rel. Brian Markus v. Aerojet Rocketdyne, Inc.*,[1] the relator, a former senior director of cybersecurity for the defendant, alleged that the company had entered into contracts with NASA and the DoD despite knowing it was not in full compliance with the contracts' cybersecurity requirements. The plaintiff's False Claims Act allegations were based on two related legal theories – implied false certification and promissory fraud, also known as fraud in the inducement. Citing the Supreme Court's opinion in *Universal Health Servs., Inc. v. United States ex rel. Escobar*,[2] the court characterized the first ground as an allegation that the company's "failure to disclose noncompliance with material statutory, regulatory or contractual requirements makes those representations misleading half truths." As for the promissory fraud count, the court described liability as attaching "to each claim submitted to the government under a contract, when the contract . . . was originally obtained through false statements or fraudulent conduct."

Consistent with the general trend of post-*Escobar* case law, the company moved to dismiss the suit on the basis that the government's actions and inactions demonstrated that the relator's claims did not satisfy the False Claims Act's materiality standard. Prior to award of the

contracts, the company had disclosed it did not comply with all parts of the applicable cybersecurity regulations, yet NASA and the DoD awarded the contracts to the company anyway. For this reason, the company argued, any noncompliance was not material under the *Escobar* standard. While the court acknowledged that the company may have disclosed some of its noncompliance, it held that the relator had met his burden of alleging with sufficient particularity that the company had made only partial disclosures. The court opined that the government agencies might not have awarded the contracts at issue if they had been aware of the full extent of the company's noncompliance.

The court went on to reject the company's second argument that the government's decision to continue the contracts in question following the filing of relator's complaint indicated acquiescence. Instead, the court stated that the appropriate inquiry is whether the "alleged misrepresentations were material at the time the government entered into or made payments on the relevant contracts." The court also rejected the notion that the government's failure to intervene in the False Claims Act case amounted to an assessment of the merits of the case in the company's favor. In addition, the court overruled the company's claim that, because cybersecurity was not the central purpose of the NASA and DoD contracts (which pertained to missile defense and rocket engine technology), any noncompliance was immaterial. Rather, the court held, the cybersecurity requirements were mandated via DoD and NASA acquisition regulations. Noncompliance could have made the company ineligible to handle sensitive technical information and thus influenced the extent to which the company could perform the required work.

The company's final argument for dismissal described the frequent amendments to DoD cybersecurity regulations in the 2013-2015 timeframe, particularly the relaxation of requirements to ease burdens on industry. Those changes, the company contended, meant that the government never actually expected full technical compliance with cybersecurity requirements. The court disagreed, holding that "[e]ven if the government never expected full technical compliance, relator properly pleads that the extent to which a company was technically compliant still mattered to the government's decision to enter into a contract."

In addition to embodying a narrow application of the *Escobar* materiality standard, the case drives home the reality that contractors and subcontractors that are subject to the government's myriad cybersecurity requirements cannot take their compliance obligations lightly. The Government Accountability Office has already affirmed that cybersecurity compliance can be a relevant factor in contract award. *See, e.g.*, *Avosys Tech., Inc.*, B-415716.6

(July 30, 2018); *Jardon and Howard Technologies, Inc.*, B-415330.3; B-415330.4 (May 24, 2018). DoD and other agencies have also made it clear that they expect compliance with the safeguarding and network penetration requirements of their cybersecurity regulations. For example, late last year, DoD issued guidance to clarify how it will communicate its cybersecurity expectations to contractors and assess their compliance with those expectations. The White House's recent National Cybersecurity Strategy document discusses the need to strengthen federal contractor cybersecurity.

In short, cybersecurity is an issue that is not going away. Government contractors and subcontractors that do not take immediate steps to assess and secure their IT systems may soon find themselves excluded from competitions, or at the wrong end of a False Claims Act lawsuit. Given that penalties under the False Claims Act can include treble damages, which might apply to the full proceeds of a contract under a fraud in the inducement theory, the cost of not implementing cybersecurity protocols could far exceed the cost of compliance.

[1] No. 2:15-CV-2245 WBS AC, 2019 WL 2024595 (E.D. Cal. May 8, 2019).

[2] 136 S. Ct. 1989 (2016).

**David Allman is a Law Clerk in the Washington, D.C. office and is not admitted to the bar.*

United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.

Decided May 8, 2019

WILLIAM B. SHUBB UNITED STATES DISTRICT JUDGE

MEMORANDUM & ORDER RE: DEFENDANTS' MOTION TO DISMISS RELATOR'S SECOND AMENDED COMPLAINT, STAY PROCEEDINGS, and COMPEL ARBITRATION

Plaintiff-relator Brian Markus brings this action against defendants Aerojet Rocketdyne Holdings, Inc. ("ARH") and Aerojet Rocketdyne, Inc. ("AR"), arising from defendants' allegedly wrongful conduct in violation of the False Claims Act ("FCA"), 31 U.S.C. §§ 3729 et seq., and relating to defendants' termination of relator's employment. Defendants now move to (1) dismiss the Second Amended Complaint ("SAC") in part for the failure to state upon which can be granted under Federal Rule of *2 Civil Procedure 12(b)(6), (2) stay proceedings, and (3) compel arbitration.

I. Background

Relator Brian Markus is resident of the State of California. (SAC ¶ 6 (Docket No. 42).) He worked for defendants as the senior director of Cyber Security, Compliance, and Controls from June 2014 to September 2015. (Id.) Defendants ARH and AR develop and manufacture products for the aerospace and defense industry. (Id. ¶ 7.) Defendants' primary aerospace and defense customers include the Department of Defense ("DoD") and the National Aeronautics & Space Administration ("NASA"), who purchase defendants' products pursuant to government contracts. (See id.) Defendant AR is a wholly-owned subsidiary of ARH, and ARH uses AR to perform its contractual obligations. (Id. ¶ 8.)

Government contracts are subject to Federal Acquisition Regulations and are supplemented by agency specific regulations. On November 18, 2013, the DoD issued a final rule, which imposed requirements on defense contractors to safeguard unclassified controlled technical information from cybersecurity threats. 48 C.F.R. § 252.204-7012 (2013). The rule required defense contractors to implement specific controls covering many different areas of cybersecurity, though it did allow contractors to submit an explanation to federal officers explaining how the company had alternative methods for achieving adequate cybersecurity protection, or why standards were inapplicable. See id. In August 2015, the DoD issued an interim rule, modifying the government's cybersecurity requirements for contractor and subcontractor information systems. 48 C.F.R. § *3 252.204-7012 (Aug. 2015). The interim rule incorporated more cybersecurity controls and required that any alternative measures be "approved in writing prior by an authorized representative of the DoD [Chief Information Officer] prior to contract award." Id. at 252.204-7012(b)(1)(ii)(B). The DoD amended the interim rule in December 2015 to allow contractors until December 31, 2017 to have compliant or equally effective alternative controls in place. See 48 C.F.R. § 252.204-7012(b)(1)(ii)(A) (Dec. 2015). Each version of this regulation defines adequate security as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." 48 C.F.R. § 252.204-7012(a).

Contractors awarded contracts from NASA must comply with relevant NASA acquisition regulations. 48 C.F.R. § 1852.204-76 lists the relevant security requirements where a contractor stores sensitive but unclassified information belonging to the federal government. Unlike the relevant DoD regulation, this NASA regulation makes no allowance for the contractor to use alternative controls or protective measures. A NASA contractor is required to "protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure." 48 C.F.R. § 1852.204-76(a).

Relator alleges that defendants fraudulently entered into contracts with the federal government despite knowing that they did not meet the minimum standards required to be awarded a government contract. (SAC ¶ 30.) He alleges that when he started working for defendants in 2014,
4 he found that defendants' *4 computer systems failed to meet the minimum cybersecurity requirements to be awarded contracts funded by the DoD or NASA. (Id. ¶ 36.) He claims that defendants knew AR was not compliant with the relevant standards as early as 2014, when defendants engaged Emagined Security, Inc. to audit the company's compliance. (See id. at ¶¶ 43, 51-53.) Relator avers that defendants repeatedly misrepresented its compliance with these technical standards in communications with government officials. (Id. ¶ 59-64.) Relator alleges that the government awarded AR a contract based on these allegedly false and misleading statements.[1] (Id. ¶ 65.) In July 2015, relator refused to sign documents that defendants were now compliant with the cybersecurity requirements, contacted the company's ethics hotline, and filed an internal report. (Id. ¶¶ 81-82.) Defendants terminated relator's employment on September 14, 2015. (Id. ¶ 83.)

[1] In total, relator alleges that AR entered into at least six contracts with the DoD between February 2014 and April 2015 (id. ¶¶ 84-93) and at least nine contracts with NASA between March 2014 and April 2016 (id. ¶¶ 105-114).

Relator filed his initial complaint in this action on October 29, 2015. (Docket No. 1.) While the government was still deciding whether to intervene in this action, relator filed his First Amended Complaint ("FAC") on September 13, 2017. (Docket No. 22.) On June 5, 2018, the United States filed a notice of election to decline intervention. (Docket No. 25.) A few months later defendants filed a motion to dismiss, stay proceedings, and compel arbitration as to the FAC. (Docket No. 39.) In response to this motion,
5 relator filed the SAC, alleging *5 the following causes of action against defendants: (1) promissory fraud in violation of 31 U.S.C. § 3729(a)(1)(A); (2) false or fraudulent statement or record in violation of 31 U.S.C. § 3729(a)(1)(B); (3) conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C); (4) retaliation in violation of 31 U.S.C. § 3730(h); (5) misrepresentation in violation of California Labor Code § 970; and (6) wrongful termination. Defendants now move to dismiss the SAC, stay proceedings, and compel arbitration. (Docket No. 50.)

II. Motion to Dismiss

A. Legal Standard

On a Rule 12(b)(6) motion, the inquiry before the court is whether, accepting the allegations in the complaint as true and drawing all reasonable inferences in the plaintiff's favor, the plaintiff has stated a claim to relief that is plausible on its face. See Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." Id. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. A complaint that offers mere "labels

and conclusions" will not survive a motion to dismiss. Id. (internal quotation marks and citations omitted).

B. Fraud Claims under the FCA

Relator brings two claims for fraud under the FCA. These two claims impose liability on anyone who "knowingly presents, or causes to be presented, a false or fraudulent claim *6 for payment or approval," 31 U.S.C. § 3729(a)(1)(A), or "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim," id. § 3729(a)(1)(B).

Outside of the context where "the claim for payment is itself literally false or fraudulent," the Ninth Circuit recognizes two different doctrines that attach FCA liability to allegedly false or fraudulent claims: (1) false certification and (2) promissory fraud, also known as fraud in the inducement. See United States ex rel. Hendow v. Univ. of Phoenix, 461 F.3d 1166, 1170-71 (9th Cir. 2006) (citation omitted). Under a false certification theory, the relator can allege either express false certification or implied false certification. The express false certification theory requires that the claimant plainly and directly certify its compliance with certain requirements that it has breached. See id. An implied false certification theory "can be a basis for liability, at least where two conditions are satisfied: first, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths." Universal Health Servs., Inc. v. United States ex rel. Escobar, 136 S. Ct. 1989, 2001 (2016). The promissory fraud approach is broader and "holds that liability will attach to each claim submitted to the government under a contract, when the contract or extension of government benefit was originally obtained through false statements or fraudulent conduct." Hendow, 461 *7 F.3d at 1173.

Under either false certification or promissory fraud, "the essential elements of [FCA] liability remain the same: (1) a false statement or fraudulent course of conduct, (2) made with scienter, (3) that was material, causing (4) the government to pay out money or forfeit moneys due." Id. Only the sufficiency of the complaint as to the materiality requirement is at issue on this motion.

[2] Defendants correctly observe that relator's FCA claims must not only be plausible but pled with particularity under Federal Rule of Civil Procedure 9(b). See Cafasso ex rel. United States v. Gen. Dynamics C4 Sys., Inc., 637 F.3d 1047, 1054-55 (9th Cir. 2011). However, defendants reference Rule 9(b) only to the extent they argue that relator has failed to plead particular facts in support of materiality. (See Mot. to Dismiss at 2-3, 15 & 18.) Therefore, the court assumes, without deciding, that relator has otherwise satisfied the requirements of Rule 9(b).

Under the FCA, a falsehood is material if it has "a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4). Most recently in Escobar, the Supreme Court clarified that "[t]he materiality standard is demanding." 136 S. Ct. at 2003. Materiality looks to the effect on the behavior of the recipient of the alleged misrepresentation. Id. at 2002. A misrepresentation is not material simply because the government requires compliance with certain requirements as a condition of payment. Id. at 2003. Nor can a court find materiality where "the Government would have the option to decline to pay if it knew of the defendant's noncompliance." Id. Relatedly, mere "minor or insubstantial" noncompliance is not material. Id. Evidence relevant to the materiality inquiry includes the *8 government's conduct in similar circumstances and whether the government has knowledge of the alleged noncompliance. See id. Defendants puts

forth four different arguments in support of their contention that relator has insufficiently pled facts as to the materiality requirement.

First, defendants argue that AR disclosed to its government customers that it was not compliant with relevant DoD and NASA regulations and therefore it is impossible for relator to satisfy the materiality prong. The Supreme Court did observe in Escobar 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." Id. Here, however, relator properly alleges with sufficient particularity that defendants did not fully disclose the extent of AR's noncompliance with relevant regulations. See id. at 2000 ("[H]alf-truths--representations that state the truth only so far as it goes, while omitting critical qualifying information--can be actionable misrepresentations."). For instance, relator alleges that AR misrepresented in its September 18, 2014 letter to the government the extent to which it had equipment required by the regulations (SAC ¶ 63), instituted required security controls (id. ¶¶ 60-61, 63), and possessed necessary firewalls (id. ¶ 62). Relator also alleges that these misrepresentations persisted over time, whereby AR knowingly and falsely certified compliance with security requirements when submitting invoices for its
9 services. *9 (Id. ¶¶ 135-36.)[3] While it may be true that AR disclosed some of its noncompliance (see id. ¶¶ 59-64), a partial disclosure would not relieve defendants of liability where defendants failed to "disclose noncompliance with material statutory, regulatory, or contractual requirements." See Escobar, 136 S. Ct. at 2001.

[3] The court recognizes that "allegations of fraud based on information and belief usually do not satisfy the particularity requirements under rule 9(b)." Moore v. Kayport Package Exp., Inc., 885 F.2d 531, 540 (9th Cir. 1989) (citation omitted). However, as explained elsewhere in this motion, there are other parts of the complaint that allege fraud with sufficient particularity for the purposes of Rule 9(b).

In fact, some of the evidence defendants put forth in favor of their motion to dismiss provides support for relator's allegations relevant to materiality.[4] The DoD informed the federal contracting officer that it could not waive compliance with DoD regulations, even for an urgent contract. (SAC ¶¶ 67-68; Req. for Judicial Notice Ex. Z at 1-4.) While the contracting officer was not prohibited from awarding the contract because of AR's noncompliance, AR could not process, store, or transmit controlled technical information until it was fully compliant. (Req. for Judicial Notice Ex. Z at 1.) Still, the DoD representative believed it to "be a relatively simple matter for the contractor to become compliant" based on the disclosure letter AR sent to the contracting negotiator. (Id. at 1-2.) Yet, relator's complaint alleges possible material nondisclosures
10 *10 in this letter, such as AR's failure to report its status on all required controls, its alleged misstatements as to partial compliance with protection measures, and the fact that the company cherrypicked what data it chose to report. (See SAC ¶¶ 59-64.)[5] Accepting these allegations as true, the government may not have awarded these contracts if it knew the full extent of the company's noncompliance, because how close AR was to full compliance was a factor in the government's decision to enter into some contracts.

4 [6] Because relator's complaint references the documents contained in defendants' Exhibits Y & Z (Docket Nos. 52-25 & 52-26) in his complaint, the court considers these materials, without converting the motion to dismiss into a motion for summary judgment, under the doctrine of incorporation by reference. See United States v. Ritchie, 342 F.3d 903, 908 (9th Cir. 2003).

[5] Defendants argue for the first time in their reply that these alleged misstatements were not associated with a claim for payment

and thus cannot support liability under the FCA. (See Reply in Supp. of Mot. to Dismiss ("Reply") at 4 (Docket No. 54).) Contrary to defendants' understanding, the FCA merely requires that the false statement(s) or fraudulent course of conduct cause the government to pay out money due. See Hendow, 461 F.3d at 1173. Under a promissory fraud theory, the relator only needs to allege that a claim was submitted "under a contract" that "was originally obtained through false statements or fraudulent conduct." See id.; see also United States ex rel. Campie v. Gilead Scis., Inc., 862 F.3d 890, 902 (9th Cir. 2017) (reaffirming Hendow's test for promissory fraud after Escobar). Here, relator alleges that AR secured its contracts with the government through misrepresentations made to government contracting agents and that the government ultimately paid out on these contracts. (See SAC ¶¶ 59-66, 129-131.)

[6] This promissory fraud theory, supported by these allegations of specific misrepresentations, distinguishes this case from United States ex rel. Mateski v. Raytheon Co., No. 2:06-CV-03614 ODW KSX, 2017 WL 3326452 (C.D. Cal. Aug. 3, 2017), aff'd, 745 F. App'x 49 (9th Cir. 2018). In Mateski, the relator merely alleged general violations of contract provisions that the government designated compliance with as mandatory to support a false certification theory. See id. at *7. Applying Escobar, the district court concluded that "such designations do not automatically make misrepresentations concerning those provisions material." Id. (citing 136 S. Ct. at 2003).

Second, defendants contend that the government's response to the investigation into AR's
11 representations *11 surrounding its cybersecurity compliance undermines relator's allegations as to materiality. Both the DoD and NASA have continued to contract with AR since the government's investigation into the allegations of this complaint. (See Req. for Judicial Notice Exs. S-V (Docket Nos. 52-19, 52-20, 52-21 & 52-22).)[7] Such evidence is not entirely dispositive on a motion to dismiss. Cf. Campie, 862 F.3d at 906 (cautioning courts not to read too much into "continued approval" by the government, albeit in a different context). Instead, the appropriate inquiry is whether AR's alleged misrepresentations were material at the time the government entered into or made payments on the relevant contracts. See Escobar, 136 S. Ct. at 2002. The contracts government agencies entered with AR after relator commenced this litigation are not at issue and possibly relate to a different set of factual circumstances. As discussed previously, relator has sufficiently alleged that AR's misrepresentations as to the extent of its noncompliance with government regulations could have affected the government's decision to enter into and pay on the contracts at issue in this case.

[7] The court GRANTS defendants' request that it take judicial notice of these exhibits. Exhibits T through V are publications on government websites and thus properly subject to judicial notice. See, e.g., Daniels-Hall v. Nat'l Educ. Ass'n, 629 F.3d 992, 998-99 (9th Cir. 2010) (finding that it is "appropriate to take judicial notice of [information on government website], as it was made publicly available by government entities [], and neither party disputes the authenticity of web sites or the accuracy of the information displayed therein."). Exhibit S is an official Authorization to Operate signed by NASA officials, so its "accuracy cannot reasonably be questioned." See Fed. R. Evid. 201(b)(2).

Defendants also argue that the government's
12 decision *12 not to intervene in this case indicates that the alleged misrepresentations were not material. (See Mot. to Dismiss at 3; Reply at 9.) As the Sixth Circuit has observed, in Escobar itself, the government chose not to intervene and the Supreme Court did not mention it as a factor relevant to materiality. See United States ex rel. Prather v. Brookdale Senior Living Communities, Inc., 892 F.3d 822, 836 (6th Cir. 2018) (citing 136

S. Ct. at 1998). Separately, "[i]f relators' ability to plead sufficiently the element of materiality were stymied by the government's choice not to intervene, this would undermine the purposes of the Act," as the FCA allows relators to proceed even without government intervention. Id. (citation omitted). And finally, there is no reason believe that the decision not to intervene is a comment on the merits of this case. See, e.g., United States ex rel. Atkins v. McInteer, 470 F.3d 1350, 1360 n.17 (11th Cir. 2006) ("In any given case, the government may have a host of reasons for not pursuing a claim."); United States ex rel. Chandler v. Cook Cty., Ill., 277 F.3d 969, 974 n.5 (7th Cir. 2002) ("The Justice Department may have myriad reasons for permitting the private suit to go forward including limited prosecutorial resources and confidence in the relator's attorney.").

Third, defendants argue that AR's noncompliance does not go to the central purpose of any of the contracts, as the contracts pertain to missile defense and rocket engine technology, not cybersecurity. See Escobar, 136 S. Ct. at 2004 n.5 (noting that a misrepresentation is material where it goes to the "essence of the bargain"). This
13 argument is unavailing at *13 this stage of the proceedings. Relator alleges that all of AR's relevant contracts with the DoD and NASA incorporated each entity's acquisition regulations. (See SAC ¶¶ 84, 105.) These acquisition regulations require that the defense contractor undertake cybersecurity specific measures before the contractor can handle certain technical information. Here, compliance with these cybersecurity requirements could have affected AR's ability to handle technical information pertaining to missile defense and rocket engine technology. (See Req. for Judicial Notice Ex. Z at 1.) Accordingly, misrepresentations as to compliance with these cybersecurity requirements could have influenced the extent to which AR could have performed the work specified by the contract.

Fourth and finally, defendants argue that the government's response to the defense industry's non-compliance with these regulations as a whole weighs against a finding of materiality. When evaluating materiality, courts should "consider how the [government] has treated similar violations." See United States ex rel. Rose v. Stephens Inst., 909 F.3d 1012, 1020 (9th Cir. 2018). Defendants contend that the DoD never expected full technical compliance because it constantly amended its acquisition regulations and promogulated guidances that attempted to ease the burdens on the industry. This observation is not dispositive. Even if the government never expected full technical compliance, relator properly pleads that the extent to which a company was technically complaint still mattered to the government's decision to enter into a contract. (See SAC ¶¶ 66-72.) Defendants have not put forth any judicially noticeable evidence that the government paid a company it knew was
14 *14 noncompliant to the same extent as AR was. Therefore, this consideration does not weigh in favor of dismissal.

Accordingly, given the above considerations, relator has plausibly pled that defendants' alleged failure to fully disclose its noncompliance was material to the government's decision to enter into and pay on the relevant contracts.

8 [8] The court expresses no opinion as to what relator will be able to establish at summary judgment or trial.

C. Conspiracy under the FCA

Relator's third count alleges that defendants participated in a conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C). Relator maintains that defendants and their officers conspired together to defraud the United States by knowingly submitting false claims. (See SAC ¶ 144.) Section 3729(a)(1)(C) imposes liability on a person who conspires to commit a violation of Section 3729(a)(1)(A) or Section 3729(a)(1)(B).

Defendants argue that this count fails as a matter of law because relator has failed to identify two distinct entities that conspired. Derived from antitrust law, the intracorporate conspiracy doctrine "holds that a conspiracy requires an agreement among two or more persons or distinct business entities." United States v. Hughes Aircraft Co., 20 F.3d 974, 979 (9th Cir. 1994) (internal quotation marks omitted). The doctrine stems from the definition of a conspiracy and the requirement that there be a meeting of the minds. See Hoefer v. Fluor Daniel, Inc., 92 F. Supp. 2d 1055, 1057 (C.D. Cal. 2000) (citing Fonda v. Gray, 707 F.2d 435, 438 (9th Cir. 1983)). While
15 *15 the Ninth Circuit has not addressed this issue, several district courts have applied the intracorporate conspiracy doctrine to FCA claims. See United States ex rel. Lupo v. Quality Assurance Servs., Inc., 242 F. Supp. 3d 1020, 1027 (S.D. Cal. 2017) (collecting cases). Courts have used this principle to bar conspiracy claims where the alleged conspirators are a parent corporation and its wholly-owned subsidiary. See, e.g., United States ex. rel. Campie v. Gilead Scis., Inc., No. C-ll-0941 EMC, 2015 WL 106255, at *15 (N.D. Cal. Jan. 7, 2015).

Here, relator identifies only a parent company, ARH, and its wholly-owned subsidiary, AR, as defendants. (SAC ¶¶ 7-8.) While relator alleges that defendants also conspired with its officers, a corporation, as a matter of law, "cannot conspire with its own employees or agents." Hoefer, 92 F. Supp. 2d at 1057. By failing to allege that defendants conspired with any independent individual or entity, relator's conspiracy claim fails as a matter of law.

Accordingly, the court will dismiss relator's third claim, that defendants participated in a conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C).

III. Motion to Compel Arbitration and Stay Proceedings

"Relator does not oppose defendants' motion to refer his employment related claims to arbitration" based on his arbitration agreement with defendants. (Opp'n to Mot. to Dismiss at 16 (Docket No. 53); see also Decl. of Ashley Neglia Ex. 1 (arbitration agreement) (Docket No. 51-1).) Relator does oppose, however, defendants' request that the entire proceedings be stayed pending the
16 resolution of these employment related claims *16 in arbitration. Relator contends that a stay is inappropriate as to his FCA claims because they are brought on behalf of the government, are not referable to arbitration, and are separate from the issues involved in his employment-related claims. (See Opp'n to Mot. to Dismiss at 16-17.)

Section 3 of the FAA provides that a court "shall on application of one of the parties stay the trial" of "any suit proceeding" brought "upon any issue referable to arbitration under [an arbitration] agreement . . . until such arbitration has been had in accordance with the terms of the agreement." 9 U.S.C. § 3. A party is only "entitled to a stay pursuant to section 3" as to arbitrable claims. Leyva v. Certified Grocers of Cal., Ltd., 593 F.2d 857, 863 (9th Cir. 1979). As to nonarbitrable claims, which defendants concede the FCA claims are, this court has discretion whether to stay the litigation pending arbitration. Id. at 863-64. This court may decide whether "it is efficient for its own docket and the fairest course for the parties to enter a stay of an action before it, pending resolution of independent proceedings which bear upon the case." Id. at 863. If there is a fair possibility that the stay may work damage to another party, a stay may be inappropriate. See Dependable Highway Exp., Inc. v. Navigators Ins. Co., 498 F.3d 1059, 1066 (9th Cir. 2007) (citation omitted).

The court will not expand the stay to encompass the nonarbitrable FCA claims. The issues involved in the FCA claims differ from those involved in relator's employment-based claims. Relator's FCA claims concern fraud that defendants allegedly perpetrated on the government, while relator's
17 employment-based *17 claims concern the alleged violation of his own rights during his employment. Resolution of relator's employment-based claims will not narrow the factual and legal issues underlying the FCA claims. While relator brings

one of his employment claims under the FCA, "[t]he elements differ for a FCA violation claim and a FCA retaliation claim." Mendiondo v. Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1103 (9th Cir. 2008). Moreover, a stay would unnecessarily work to delay resolution of relator's FCA claims, which have been pending for more than three years.

Accordingly, the court will refer relator's employment-based claims, Counts Four, Five, and Six, to arbitration and stay proceedings as to these claims only.

9 [9] All remaining Requests for Judicial Notice (Docket No. 52) are DENIED as MOOT. --------

IT IS THEREFORE ORDERED that defendants' Motion to Dismiss Relator's Second Amended Complaint (Docket No. 50) be, and the same hereby is, GRANTED IN PART. Count Three of relator's Second Amended Complaint is DISMISSED WITH PREJUDICE. The motion is DENIED in all other respects.

IT IS FURTHER ORDERED that defendants' Motion to Compel Arbitration and Stay Proceedings (Docket No. 50) be, and the same hereby is, GRANTED with respect to Counts Four, Five, and Six of relator's Second Amended Complaint. Proceedings as to Counts One and Two are not stayed. Dated: May 8, 2019

/s/_____

WILLIAM B. SHUBB

UNITED STATES DISTRICT JUDGE