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

DOD Contractor Cybersecurity Rule Brings New FCA Risks

By **Robert Metzger, Stephen Bacon and Alexandria Webb**
(October 21, 2020, 5:24 PM EDT)


Robert Metzger


Stephen Bacon


Alexandria Webb

The U.S. Department of Defense recently published an interim rule to establish new methods for assessing contractor implementation of cybersecurity requirements.[1] The interim rule presents new and significant areas of potential liability for contractors under the False Claims Act.

Most notably, the interim rule will require many contractors to conduct a self-assessment of their cybersecurity and submit, as a condition for award, a summary-level score reflecting the state of their compliance. This requirement creates FCA risks that contractors should fully understand and appreciate before the interim rule takes effect on Nov. 30, and which may require prompt action thereafter to enhance and document responsible cybersecurity measures.

Interim Rule Background

The interim rule builds upon Defense Federal Acquisition Regulation Supplement 252.204-7012.[2] This rule requires contractors to implement 110 security requirements specified by the National Institute of Standards and Technology Special Publication 800-171 to provide adequate security for their information systems that process, store or transmit covered defense information.

Under current regulations, contractors represent that they will implement these requirements by submitting an offer on a contract that is subject to the 7012 clause.[3]

The interim rule adds new clauses— DFARS 252.204-7019 and DFARS 252.204-7020 — that will provide the DOD with visibility into the extent of a contractor's actual technical compliance with the 7012 clause and NIST SP 800-171.

Under the new 7019 clause, all offerors that are required to implement NIST SP 800-171 must complete at least a basic assessment of their information systems relevant to an offer. The contractor's basic assessment results in a summary-level score of the contractor's compliance with NIST SP 800-171 — e.g., 95 out of 110.

The summary-level score is then posted to the supplier performance risk system, or SPRS, the DOD's authoritative source for supplier and product performance information.[4] A contractor that has not attained the maximum score of 110 must disclose the date it expects to achieve that score based on its current system security plan and plan of action and milestones, or POAM.

To be considered for award, where the 7019 and 7020 clauses are present, the offeror must have a current basic assessment that is not more than 3 years old, unless a shorter time is specified in the solicitation. Prior to awarding a contract, or exercising an option, contracting officers must verify that the SPRS includes a summary-level score for each covered information system that is relevant, including those of subcontractors that are subject to the NIST SP 800-171 requirements.

In a rule proposed separately, the DOD has indicated that it intends to use the information in the SPRS as a factor in determining whether a prospective contractor is "responsible" to perform.[5] This suggests — but does not confirm — that DOD procuring activities could find a contractor nonresponsible due a low summary-level score.

Understandably, facing this possibility, contractors will feel pressure to achieve a high score and some may be tempted to misrepresent the true state of their compliance or POAM plans. Contractors that succumb to this temptation may face severe consequences under the FCA.

The Basic Assessment and Potential FCA Liability

The basic assessment requirement under the interim rule could potentially implicate two distinct theories of liability under the FCA: (1) promissory fraud, also known as fraud in the inducement; and (2) false certification.

A contractor can be held liable under the promissory fraud theory if it obtains a contract or option extension through false statements or fraudulent conduct. The false certification theory encompasses express false certification and implied false certification.

Express false certification requires direct certification of compliance with certain requirements. Under the implied false certification theory, a contractor can be held liable if it makes specific representations about goods or services provided under a contract and fails to disclose noncompliance with material regulatory or contractual requirements.

At least one federal district court has considered how these theories apply to a contractor's alleged noncompliance with the 7012 clause and the security requirements specified by NIST SP 800-171.[6] In U.S. v. Aerojet Rocketdyne Holdings Inc., the relator, a former Aerojet employee who was responsible for cybersecurity, brought a qui tam action against Aerojet under the FCA. He alleged that Aerojet misrepresented its compliance with cybersecurity requirements to fraudulently obtain contracts with the government. The relator also claimed he was wrongfully terminated in retaliation for his refusal to certify Aerojet's compliance with cybersecurity requirements.

Aerojet moved to dismiss the complaint on the basis that the relator failed to plausibly allege the element of materiality required under the FCA. The U.S. District Court for the Eastern District of California disagreed with Aerojet's position and held that the relator sufficiently alleged materiality because he claimed Aerojet "did not fully disclose the extent of [its] noncompliance with relevant regulations."[7]

Although Aerojet argued that the government did not expect full compliance with all cybersecurity requirements, the court concluded that the relator plausibly alleged "that the extent to which a company was technically compliant still mattered to the government's decision to enter into a contract."[8]

The Aerojet decision foreshadows several types of potential FCA actions that could be filed against contractors in connection with the basic assessment requirement. It also suggests companies will find little protection if they contend that the government would have awarded the contract even if it had known the true facts of imperfect cyber compliance.

False or Misleading Summary-Level Scores

FCA actions will likely be filed against contractors that submit a false or misleading summary-level score that does not reflect the true extent of their compliance with NIST SP 800-171. FCA plaintiffs — the government or qui tam relators — may allege that an inaccurate summary-level score is material to the DOD's decision to enter into a contract.

They may argue that the government relies on the accuracy and truthfulness of the information in the SPRS — including the summary-level score and the date that the contractor expects to achieve a score of 110 — to make an affirmative responsibility determination that is a prerequisite for a contract award. The Aerojet decision suggests that such allegations may be sufficient to form the basis for a viable FCA action that can at least survive a motion to dismiss, and proceed with costly and time-consuming discovery.

As contractors complete basic assessments of their information systems, they should take prudent steps to avoid or neutralize potential FCA allegations. At a minimum, contractors should maintain all documentation associated with their basic assessments, including system security plans and POAMs, assessment plans and procedures, documentation supporting selection of assessment methods and objects, and evidence — including self-assessment reports — that was considered to determine whether a security requirement is satisfied or not.

Contractors should respect and respond to any internal differences of opinion regarding whether certain requirements are satisfied. A contractor's rationale for its final scoring determination for each requirement should also be well-supported and well-documented.

Further, should it have sufficient resources, a contractor might consider using an independent third-party assessment to support the sufficiency and accuracy of its self-assessment. Protective measures such as these could help contractors defend against FCA claims based on alleged cybersecurity noncompliance by showing that they acted reasonably and in good faith in completing their basic assessment obligation.

Failure to Make a Good Faith Effort to Achieve a Score of 110

Contractors could also face potential FCA liability if they fail make a good faith effort to achieve a score of 110 after the basic assessment is completed.

For example, suppose a contractor completes a basic assessment and submits a summary-level score of 90 that is posted to the SPRS on Dec. 1. The contractor's SPRS data also represents that it expects to achieve a score of 110 by July 1, 2021.

On Jan. 1, 2021, the DOD awards the contactor a one-year contract with four one-year options. However, the contractor fails to follow its POAM to correct deficiencies and does not achieve a score of 110 by July 1, 2021. Subsequently, the DOD exercises the first option year on Jan. 1, 2022, without knowledge that the contractor's score remains unchanged at 90.

The DOD could learn — through a whistleblower, Defense Contract Management Agency audit, or damage assessment following a cyber incident — that the contractor did not, in fact, correct its cybersecurity deficiencies as promised. In those situations, the contractor could face FCA liability for withholding information from the DOD about its noncompliance, and failing to execute POAMs in good faith to achieve a score of 110 on the timeline reflected in the SPRS.

A contractor's failure to disclose its noncompliance in this situation could arguably be material if it can be shown that the DOD's knowledge of the noncompliance would have influenced its decision to exercise the option or continue paying the contractor. The threat of this kind of FCA action underscores the need for contractors to submit realistic dates by which they can achieve a score of 110 and, once the basic assessment is completed, to faithfully execute their POAMs and document the steps they have taken to fix compliance gaps.

Failure to Update Materially Inaccurate SPRS Data

FCA allegations could also be based on a contractor's failure to update their basic assessment as may be appropriate prior to the award of a contract. Under the 7019 clause, offerors are required to "verify that summary-level scores of a current NIST SP 800-171 DOD assessment — i.e., not more than 3 years old unless a lesser time is specified in the solicitation — are posted in [SPRS] for all covered contractor information systems relevant to the offer."[9]

This suggests that a contractor need only complete a basic assessment once every three years to be eligible for award as long as a so-called current summary-level score is posted in the SPRS. The interim rule does not state that contractors must update their basic assessment with each offer, nor does it explicitly require contractors to verify the accuracy of the information in the SPRS prior to each offer.

There could be circumstances, however, where an offeror's summary-level score in the SPRS is misleading such that failing to update it could arguably be considered a material misrepresentation in violation of the FCA.

For example, suppose in the scenario described above that the contractor submits an offer on Aug. 1, 2021, in response to a DOD solicitation. As required under the interim rule, the contracting officer verifies that the contractor has a summary-level score of a current basic assessment in the SPRS (posted on Dec. 1) and proceeds to award the contract to the contractor on Sept. 1, 2021.

Based on the information in the SPRS, the contracting officer might reasonably assume at the time of award that the contractor has already achieved a score of 110 by its expected completion date (July 1). If circumstances change and the contractor's security were to erode, or even if its score remains unchanged at 90, the contractor could face FCA claims based on its failure to update the information in the SPRS and/or disclose its incomplete compliance to the contracting officer prior to award.

Over the three-year term of a basic assessment, it seems more likely than not that achievement of SP 800-171 requirements will change. Companies with relatively low initial summary-level scores will be

motivated to improve their security and report improved scores. They should be encouraged and enabled to do so.

FCA Defendants Face Significant Liability

Contractors that misrepresent the results of a basic assessment are vulnerable to civil or criminal liability under the FCA. The FCA provides for treble damages, calculated by multiplying the government's loss by three, in addition to steep civil penalties that can exceed $23,000 per violation.

Moreover, if a contractor engages in fraud in the inducement, FCA liability attaches to each claim for payment submitted under the fraudulently obtained contract. Thus, in an action that alleges fraud in the inducement, the government will often seek damages totaling three times the value of the fraudulently obtained contract.

The prospect of significant criminal and civil FCA liability should deter contractors from reporting false or misleading information in connection with the basic assessment requirement.

Recommendations

The interim rule does not specify what action, if any, a contractor must take if it does not achieve a score of 110 by the date listed in the SPRS. Nor is it clear under what circumstances a contractor may report an improved or changed summary-level score.

The final rule should be clarified so that contractors are provided clear direction regarding whether, and under what circumstances, the DOD must be notified if the planned completion date is not achieved or if a contractor's summary-level score improves or otherwise changes. Contractors should also know when it is recommended, or even required, to conduct and report a new self-assessment.

In the absence of further clarity, contractors should consider whether to notify the DOD contracting officers if they do not meet the planned completion date or if their summary-level scores otherwise change. Such a notification could explain how a summary score has changed or, in the case of a contractor's failure to meet its planned completion date, why the contractor was unable to achieve the score of 110 by the planned completion date and what additional steps the contractor will take to correct any remaining deficiencies.

Conclusion

A recent DOD inspector general report indicates that the DOD is well aware that many contractors do not consistently implement all of the security requirements specified by NIST SP 800-171.[10] As increasing numbers of contractors post their summary-level scores on the SPRS, the DOD will know much more about the deficiencies and plans of individual contractors.

The basic assessment requirement will create a positive incentive for contractors to bolster their cyber defenses, while informing the DOD who has gaps and when they are to be mitigated.

Obtaining the maximum score of 110 will be challenging and costly for many companies, particularly small businesses. Some companies may resort to shortcuts, misrepresentations or outright falsehoods in order to check the box created by the new basic assessment requirement.

Those who do will face not only potentially devastating liability under the FCA, but also contractual consequences, e.g., the threat of a termination for default, breach of contract claim, suspension or debarment action and adverse past-performance ratings.

Contractors must manage cybersecurity and implementation of NIST SP 800-171 with these potential legal ramifications in mind. These imperatives are present realities because the new 7019 and 7020 contract clauses will appear in DOD solicitations and contracting actions once the interim rule becomes effective on Nov. 30.

Robert S. Metzger is a a partner at Rogers Joseph O'Donnell PC and a co-author of the MITRE Corporation "Deliver Uncompromised" Report, which contributed to the DOD's Cybersecurity Maturity Model Certification initiative.

Stephen L. Bacon is an associate at Rogers Joseph.

Alexandria Tindall Webb is of counsel at the firm.

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 85 Fed. Reg. 61,505 (Sept. 29, 2020).

[2] https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

[3] See DFARS 252.204-7008.

[4] https://www.sprs.csd.disa.mil/.

[5] See 85 Fed. Reg. 53,748 (Aug. 31, 2020).

[6] See U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019).

[7] Id. at 1246.

[8] Id. at 1249.

[9] DFARS 252.204-7019(c).

[10] See DODIG-2019-105, Audit of Protection of DOD Controlled Unclassified Information on Contractor-Owned Networks and Systems (July 23, 2019).