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's New Cyber Rules May Spur Contract Disputes

By **Robert Metzger, Stephen Bacon and Alexandria Webb**
(February 22, 2021, 4:17 PM EST)

Robert Metzger

Stephen Bacon

Alexandria Webb

Last year, the U.S. Department of Defense published an interim rule to establish new methods for assessing contractor implementation of cybersecurity requirements.[1]

The interim rule will require thousands of defense contractors to conduct at least a basic assessment of their compliance with the 110 security requirements specified by the National Institute of Standards and Technology Special Publication 800–171.

The interim rule will prompt potential contact disputes, as could involve terminations for default, payment reductions for noncompliance, challenges to DOD cybersecurity assessments and monetary claims.

Contractors now are receiving solicitations and contracts with new Defense Federal Acquisition Regulation Supplement clauses 252.204-7019 and 252.204-7020, which implement the new cyber requirements. Contractors should recognize these potential areas of dispute.

Interim Rule Background

Under the DFARS 252.204-7012 compliance clause, in place for several years, contractors are to implement NIST SP 800–171 measures to provide adequate security for their covered information systems that process, store and transmit covered defense information.

Before the interim rule took effect, contractors had only to represent that they would implement NIST SP 800–171 by submitting an offer on a contract that is subject to the 7012 clause.[2]

Under the new 7019 clause, however, to be eligible for award, offerors who are required to implement NIST SP 800-171 must complete at least a basic assessment of their information systems relevant to an offer and must submit a summary-level score of that assessment to the DOD.

Summary level scores — e.g., 90 out of 110 — are posted in the supplier performance risk system, or SPRS. A contractor that has not attained the maximum score of 110 must disclose the date that it expects to achieve that score based on its current system security plan and its plan of action and milestones.

The DOD contracting officers must check the SPRS to verify that contractors have a summary level score that is current — not more than three years old — prior to contract award and prior to exercising an option.[3]

Once a contract is awarded that includes the 7020 clause, the DOD may, at its discretion, conduct a medium or high assessment of covered information systems that are subject to NIST SP 800–171.[4] These are conducted by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center.[5]

Terminations for Default

A default termination is a drastic sanction that can have devastating consequences for contractors.[6] If the termination is justified, the government may recover unliquidated progress payments, excess costs to reprocure the same items or services, and other damages arising from the contractor's failure to perform.

Noncompliance with NIST SP 800–171 could be grounds for the DOD to terminate a contract for default. Should a severe cyber incident occur during contract performance, the DOD may investigate. The DOD could determine that the contractor's actual cybersecurity was materially different from that suggested by the score it posted on the SPRS.

Similarly, in the course of a medium or high assessment, the DOD might learn that a contractor has poorer security than what it reported on the SPRS, or that it has failed to make progress to meet its stated plan-of-action-and-milestones completion date.

In such event, the DOD might assert that a contractor's failure to implement NIST SP 800–171, as required under the 7012 clause, is a failure to perform "any of the other provisions of th[e] contract" under subsection (a)(1)(iii) of the standard default clause.[7]

There has been at least one reported case from the U.S. Armed Services Board of Contract Appeals, or ASBCA, in which the DOD has terminated a commercial item contract for cause under FAR 52.212-4(m) because the contractor allegedly failed to comply with NIST SP 800–171.

In Arcade Travel Inc., the DOD terminated three contracts for travel management services after a cybersecurity investigation revealed that the contractor was not in compliance with NIST SP 800–171.[8]

The DOD also asserted an affirmative claim against the contractor seeking $311,700 in costs the DOD incurred for credit monitoring services as a result of a related data breach that impacted the contractor's information systems.

Although the ASBCA has not yet ruled finally on the case, Arcade Travel should alert contractors that they can face significant consequences for failing to comply with NIST SP 800–171.

Contractors also could be terminated for default if the DOD learns that they misrepresented the state of

their compliance with NIST SP 800–171 at the time of award.[9] Fraudulent misrepresentations may render a contract void from the inception and justify the government's decision to default the contract and/or pursue False Claims Act allegations.[10]

Prime contractors are generally responsible for the performance of their subcontractors.[11] The DOD lacks privity of contract with subcontractors, looks to prime contractors to flow down cyber requirements and expects measures to determine that subcontractors have adequate security.[12]

This underscores the need for prime contractors to vet and select responsible subcontractors who commit to and can demonstrate cybersecurity compliance.[13] If the DOD were to hold a prime liable for the cyber faults of a subcontractor, one can expect the prime to seek redress from the sub under cyber clauses that flow down or on indemnity theories.

Payment Reductions

Contracts that include FAR 52.232-16 — on progress payments — permit the contracting officer to reduce or suspend progress payments if the contractor failed to comply with any material requirement of the contract or if performance of the contract is endangered by the contractor's failure to make progress.[14]

Where a contractor fails to comply with NIST SP 800–171 or fails to make progress toward its plan-of-action-and-milestones completion date, a DOD contracting officer could demand corrective action and threaten to or actually suspend, or reduce, the contractor's progress payments.[15]

The DOD also might attempt to unilaterally reduce the value of a contract on the basis that services performed by a contractor were defective due to noncompliance with the 7012 clause.

Although it would be difficult to reasonably quantify the reduction in value attributable to the noncompliance, the DOD might use that contractual remedy to penalize a contractor for failing to comply with NIST SP 800–171.

Challenging Defense Industrial Base Cybersecurity Assessment Center Assessment Results

NIST SP 800–171 states 110 requirements, each of which is potentially susceptible to different interpretations or varying applications. Accordingly, the risk is real that the government will disagree with how a contractor addressed, and whether it is compliant with, particular cyber requirements.

Potentially, a contractor may contest the final result of a medium or high assessment at the ASBCA or U.S. Court of Federal Claims under the Contract Disputes Act.[16] Such a challenge could proceed much like a challenge to a contractor performance assessment report, or CPAR.

Precedent on CPAR cases suggests that the claims court and the ASBCA have CDA jurisdiction to determine whether the contracting officer acted arbitrarily and capriciously in accepting or acting upon an inaccurate and unfair performance evaluation.[17]

While the court and the ASBCA lack authority to direct the contracting officer, or the Defense Contract Management Agency, to issue a specific assessment result, they can remand the matter to require that the contracting officer follow the applicable regulations and provide the contractor the benefit of a fair and accurate evaluation.[18]

Claims for Equitable Adjustment

The DOD's position, expressed many times, is that the 7012 clause has been included in defense contracts, and flowed down, for years.[19]

The DOD is therefore unwilling to pay additional costs for cyber measures which, in their view, already should have been accomplished by contractors who previously attested by their bids that they were in compliance with the 7012 clause.

However, there are new requirements present in the new 7019 and 7020 DFARS clauses, and these will not be present in contracts awarded before Nov. 30, 2020, the effective date of the interim rule.

Conceivably, contractors could seek equitable adjustment if the government imposes these clauses by unilateral modification and where costs result that were not priced in the contract as awarded.

Relatedly, the government could demand cyber measures which are beyond that reasonably necessary under a contractor's interpretation of the DFARS and NIST SP 800-171 requirements. This also could generate contractor claims under the standard "Changes" clause included in all government contracts.[20]

Similarly, the DOD should not seek to impose unilaterally the 7019 or 7020 clauses as a condition to exercising an option on a contract awarded prior to the effective date of the interim rule.

Attempts by the government to alter the conditions of the contractor's existing obligations, for example by adding the 7019 or 7020 clauses or other cyber demands, could invalidate its ability to exercise an option.[21] This suggests that, if the DOD decides to add the new interim rule clauses to an existing contract, it should do so by bilateral contract modification.

Conclusion

The interim rule imposes new and significant cyber obligations on thousands of defense suppliers. Contractors should implement its requirements promptly and capably, accurately self-assess and submit their cyber scores to the SPRS, stay on their plan-of-action-and-milestones schedule, and ensure that internal documentation aligns with their SPRS submissions.

Contractors should never misrepresent their cyber status or overpromise when they will close known gaps. Contractors should also take continuous measures to monitor and improve their security, because the best way to avoid cyber compliance disputes is to have systems, practices and processes that will avoid compromise, mitigate consequence and facilitate prompt reporting should a breach nevertheless occur.

Robert S. Metzger is a shareholder, Stephen L. Bacon is an associate and Alexandria Tindall Webb is of counsel at Rogers Joseph O'Donnell PC.

[1] See 85 Fed. Reg. 61,505 (Sept. 29, 2020).

[2] DFARS 252.204-7008(c)(1).

[3] DFARS 204.7303. Contracting officers are likely to check only the score of a contractor who is in line to receive a prime contract award, however, not their subcontractors.

[4] DFARS 252.204-7020(c). Only a very small percentage of the contractors subject to the 7020 clause will be subject to either a medium or high assessment, however, owing to the limited Defense Industrial Base Cybersecurity Assessment Center resources.

[5] After the Defense Industrial Base Cybersecurity Assessment Center completes a medium or high Assessment, the contractor has "14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question." DFARS 252.204-7020(e)(2).

[6] Lisbon Contractors Inc. v. United States, 828 F.2d 759, 765 (Fed. Cir. 1987) (citations omitted).

[7] See FAR 52.249-8(a)(1)(iii). Before it can exercise this right, the government must provide notice and opportunity to cure within 10 days — a very short period to resolve significant cyber shortfalls.

[8] See Arcade Travel Inc. d/b/a Boersma Travel Servs., ASBCA No. 62009, 20-1 BCA ¶ 37,641. A termination for cause is permitted under the standard commercial item FAR clause "if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance." FAR 52.212-4(m).

[9] The government also may assert fraud-in-the-inducement as an affirmative defense to legitimate monetary claims. See, e.g., Laguna Construction Co. v. Carter, 828 F.3d 1364, 1370 (Fed. Cir. 2016). To the extent a contractor makes a fraudulent misrepresentation in connection with a claim, it is also at risk of forfeiture. See 28 U.S.C. § 2514; 41 U.S.C. § 7101(9).

[10] See, e.g., Vertex Construction & Engineering, ASBCA No. 58988, 14-1 BCA ¶ 35,804 (default upheld where contractor submitted a fraudulent master electrician certificate in order to secure the contract).

[11] See Johnson Mgm't Grp. CFC, Inc. v. Martinez, 308 F.3d 1245, 1252 (Fed. Cir. 2002) ("A contractor is responsible for the unexcused performance failures of its subcontractors.").

[12] DOD, Def. Cont. Mgmt. Agency, Contractor Purchasing Sys. Rev. Guidebook, Appendix 24 (June 14, 2019), https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_062719.pdf.

[13] Supplier Performance Risk System scores are unavailable to Department of Defense primes. Thus, subcontractors with access to high value information on sensitive programs can expect primes to ask for disclosure of SPRS scores and for other verification of adequate cyber measures.

[14] FAR 52.232-16(c).

[15] Under FAR 52.246-4 on inspection of services, the government may "reduce the contract price to reflect the reduced value of the services performed" in situations where "the defects in services cannot

be corrected by reperformance." This could be applied to deficiencies in the performance of cyber obligations, but determination of the changed value of services would be difficult.

[16] See generally 41 U.S.C. § 7104.

[17] See Todd Constr. LP v. U.S., 656 F.3d 1306, 1316 (Fed. Cir. 2011); MicroTechnologies LLC, ASBCA Nos. 59911, 59912, 16-1 BCA ¶ 36,354 at 177,236.

[18] See, e.g., PROTEC GmbH, ASBCA No. 61161 et al., 18-1 BCA ¶ 37,064 at 180,419-20 (Although the board does not have "jurisdiction to order an agency to revise a CPARS rating," it is permitted to "remand a matter to require a CO to follow applicable regulations and provide appellant with a fair and accurate performance evaluation."); Versar Inc., ASBCA No. 56857, 10-1 BCA ¶ 34,437 at 169,959 (The board does not possess "jurisdiction to grant specific performance or injunctive relief.").

[19] The DFARS 252.204-7012 (October 2016) required contractors to implement NIST SP 800-171 not later than Dec. 31, 2007.

[20] See, e.g., FAR 52.243-1, Changes-Fixed Price.

[21] See, e.g., Varo Inc., ASBCA No. 47945, 96-1 BCA ¶ 28,161.