# PRATT'S GOVERNMENT CONTRACTING LAW REPORT

**VOLUME 6** **NUMBER 12** **December 2020**



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at ..... 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)
ISSN: 2688-7290

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt).
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub.4938)

# *Editor-in-Chief, Editor & Board of Editors*

*Pratt's Government Contracting Law Report* is published 12 times a year by Matthew Bender & Company, Inc.  For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

# Department of Defense Overhauls Contractor Information Security Requirements Through Its Interim Rule Implementing the CMMC and DoD NIST SP 800-171 Assessment Methodology

***By Thomas Pettit, Ronald D. Lee, Charles A. Blanchard, and Tom McSorley****

*The Department of Defense issued an interim rule creating three new information security Defense Federal Acquisition Regulation Supplement clauses, which implement two new cybersecurity programs: the Cybersecurity Maturity Model Certification and the National Institute of Standards and Technology Special Publication 800-171 Assessment Methodology. The authors of this article discuss the interim rule.*

The Department of Defense ("DoD") issued an interim rule[1] (the "Interim Rule") creating three new information security Defense Federal Acquisition Regulation Supplement ("DFARS") clauses:

- DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*;
- DFARS 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*; and
- DFAR 252.204-7021, *Cybersecurity Maturity Model*.[2]

These clauses implement two new cybersecurity programs: the Cybersecurity Maturity Model Certification ("CMMC") and the National Institute of

* Thomas Pettit (thomas.pettit@arnoldporter.com) is a government contracts associate at Arnold & Porter Kaye Scholer LLP representing clients across industry sectors facing a range of government contracting challenges, including litigation, cybersecurity, transactions, and investigations. Ronald D. Lee (ronald.lee@arnoldporter.com) is a partner at the firm advising and representing clients in national security, cybersecurity and privacy, and government contracts matters. Charles A. Blanchard (charles.blanchard@arnoldporter.com), a partner at the firm who previously served as the General Counsel of the Air Force and the Army, works with clients in the contracting and national security communities, providing unique insights into doing business with the federal government. Tom McSorley (tom.mcsorley@arnoldporter.com) is a senior associate at the firm advising clients on the intersection of law, technology, national security, and foreign policy.

[1] https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

[2] 85 Fed. Reg. 61505 (Sept. 29, 2020) ("Interim Rule").

Standards and Technology ("NIST") Special Publication ("SP") 800-171 Assessment Methodology. Those programs will overhaul DoD's cybersecurity regime by imposing new assessment and certification requirements on prime contractors and subcontractors throughout the supply chain for all acquisitions and contracts, except those solely for commercial-off-the-shelf ("COTS") items.[3]

Notably, the Interim Rule's preamble indicates that these clauses will apply only to procurements that exceed the micro-purchase threshold, but the implementing DFARS sections[4] do not contain that limitation.

The Interim Rule took effect on November 30, 2020.[5] DoD has decided to implement the Interim Rule "without prior opportunity for public comment" pursuant to 41 U.S.C. § 1707(d) and FAR 1.501-3(b) to address what it perceives as an "urgent and compelling" need to protect sensitive DoD information.[6] Although the Interim Rule took effect on November 30, DoD is using a phased approach to implement both the CMMC and the NIST SP 800-171 Assessment Methodology. DoD will incorporate the CMMC into solicitations and contracts over a five-year period, targeting an October 1, 2025 full implementation date.[7] Notwithstanding the phased implementation (and prior DoD statements), nothing in the Interim Rule expressly precludes DoD from amending existing contracts to incorporate these programs or limits the number of acquisitions that can include these clauses prior to October 1, 2025. This is particularly true with respect to the CMMC. The Interim Rule's preamble suggests that DoD will implement the NIST SP 800-171 Assessment Methodology by incorporating that program into "new" solicitations and contracts, but it does not similarly limit the CMMC.[8]

We note that these new requirements are implemented in new contract clauses that do not supplant DFARS 252.204-7012, which remains in effect and which will continue to establish the baseline security requirements

---

[3] *Id.* at 61506 ("CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025.").

[4] DFARS 204.7304(d)–(e).

[5] *Id.* at 61506.

[6] *Id.* at 61517.

[7] *Id.* at 61506.

[8] *Id.* at 61509, 61510.

applicable to most DoD contracts. Any member of the public interested in filing comments had to do so no later than November 30, 2020.[9]

## NIST SP 800-171 ASSESSMENT METHODOLOGY

In February 2019, the Under Secretary of Defense for Acquisition and Sustainment instructed the Defense Contract Management Agency ("DCMA") to create a program for assessing defense contractors' compliance with and implementation of the 110 security controls reflected in NIST SP 800-171 under contracts subject to DFARS 252.204-7012, which applies to contractors with information systems that will store, process, or transmit controlled unclassified information ("CUI"). This directive stemmed from DoD concerns over what it perceived as the failure of defense contractors subject to DFARS 252.204-7012 to timely implement the NIST SP 800-171 security controls.[10]

Underlying these concerns is DoD's observation that the current DFARS 252.204-7012 information security regime relies upon contractor self-assessments and, in some respects, is a documentation exercise. NIST SP 800-171 requires offerors to develop system security plans ("SSPs") detailing how contractors have implemented NIST SP 800-171 security controls, but offerors are not required to implement all 110 controls to be compliant. Rather, offerors may develop plans of action ("POAs") identifying controls not implemented and how they have mitigated the risks associated with not having implemented those controls.[11] Contractors are expected to execute their POAs to implement all applicable 110 NIST SP 800-171 security controls, but there are no firm timing requirements for doing so. Nor is there any mandatory government oversight. Recent questionnaires and surveys have indicated that defense contractors are not consistently and timely executing their POAs.[12]

---

[9] *Id.* at 61505.

[10] *Id.* at 61509, 61518.

[11] NIST SP 800-171 Rev.2 at 47, https://doi.org/10.6028/NIST.SP.800-171r2.

[12] Interim Rule at 61518. A 2017 questionnaire revealed that defense contractors and subcontractors had "implementation rates of 38% to 54% for at least ten of the 110 security requirements of NIST SP 800-171." *Id.* (citing *Complying with NIST 800-171*, Aerospace Industries Association). In a "2018 survey, 36% of contractors who responses indicated a lack of awareness of DFARS clause 252.204-7012 and 45% of contractors acknowledged not having read NSIT SP 800-171. *Id.* (citing *Implementing Cybersecurity in DoD Supply Chains*, National Defense Industrial Association ("NDIA") (July 2018)). A 2019 survey revealed that only 56% of defense contractors were prepared for a DCMA assessment of NIST SP 800-171 compliance. *Id.* (citing *Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy*, NDIA (October 2018) at 20, 24).

In response, DCMA created the NIST SP 800-171 Assessment Methodology,[13] which DoD is implementing through new DFARS clauses 252.204-7019 and -7020. Pursuant to those clauses, contracting officers must incorporate the NIST SP 800-171 Assessment Methodology into all solicitations and contracts that exceed the micro-purchase threshold and are not exclusively for the acquisition of COTS items.[14]

**Assessment Overview**

The NIST SP 800-171 Assessment Methodology consists of two components: a weighted score and a confidence level in the score. With respect to score, the assessment establishes a 110-point, weighted scoring system to measure the extent to which an offeror or contractor has implemented the NIST SP 800-171 security controls.[15] The assessment provides a standardized scoring methodology that assigns greater points to requirements that "have more impact on the security of the network and its data than others."[16]

For instance, security controls designed to "limit system access to authorized users" are critical to protecting information systems, and failing to implement those controls will limit the effectiveness of other controls.[17] Accordingly, they are worth more points than other less critical controls.[18]

The assessment establishes three confidence levels that "reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment."[19] These confidence levels are tied to the type of assessment performed. A Basic Assessment refers to "a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government."[20] A Basic Assessment means there is a Low level of confidence in the score, as it is self-generated.[21] For a Medium Assessment, the government reviews a contractor's Basic Assessment and associated documen-

---

[13] https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

[14] DFARS 204.7304(d)-(e) (Interim Rule at 61519).

[15] NIST SP 800-171 DoD Assessment Methodology Version 1.2.1 at 6, https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Interim Rule at 61505.

[20] *Id.*; *see also* DFARS 252.204-7020(a) (*id.* at 61521).

[21] DFARS 252.204-7020(a) (*id.* at 61521).

tation and discusses any concerns with the contractor.[22] This results in a "Medium" level of confidence in the score.[23]

A High Assessment not only requires the government to review the contractor's Basic Assessment and associated documentation but also requires "[v]erification, examination, and demonstration" of the contractor's SSP to validate that the contractor has in fact implemented the NIST SP 800-171 controls as stated in the SSP.[24] This assessment results in a "High" level of confidence in the resulting score.[25] If the contractor disagrees with any government findings in connection with a Medium or High Assessment, it has the right to "rebuttal and adjudication."[26]

The Interim Rule does not define the "adjudication" process, but a contractor will at a minimum be allowed to provide additional information within "14 business days" of the government's assessment "to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question." [27]

Information relating to these assessments will be stored in the Supplier Performance Risk System ("SPRS").[28] Specifically, the SPRS will provide the summary level scores, type of assessment, a description of the SSP architecture, the date of assessment, and the date by which the contractor will achieve a full score of 110.[29]

**Proposal and Contract Requirements**

If a DoD solicitation or contract requires the contractor to comply with NIST SP 800-171, the contracting officer—prior to awarding the contract or exercising a contract extension—must review the SPRS to verify that the offeror has a "current assessment (i.e., not more than 3 years old unless a lesser time is

---

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] DFARS 252.407-7020(e) (Interim Rule at 65122).

[27] DFARS 252.407-7020(e)(2) (Interim Rule at 65122).

[28] The SPRS will be available to all DoD components and will not be publicly available. Offerors/contractors will be able to view their own information in the SPRS. DFARS 252.204-7019(d)(3) (Interim Rule at 61521). Prime contractors will not be able to review assessment information for subcontractors and thus will need to ask subcontractors to provide information from the SPRS.

[29] DFARS 252.204-7019(d)(1) (Interim Rule at 61521-22); DFARS 252.204-7020(d)(1) (Interim Rule at 61522).

specified in the solicitation) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order."[30]

Contracting officers must verify that offerors contractors subject to DFARS 252.204-7012 have a current NIST SP 800-171 assessment and "summary level score" in the SPRS at the time of award[31] and prior to exercising options for all procurements and contractors incorporating DFARS 252.204-7019 and -7020. An assessment is "current" if it is no more than three years old at the time of award or contract action.[32]

Prime contractors and higher-tier subcontractors must incorporate DFARS 252.204-7020 into all subcontracts other than those for COTS items.[33] Prior to awarding any subcontract, the prime contractor or higher-tier subcontractor must verify that "the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment . . . for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government."[34]

**DFARS 252.204-7021 AND THE CMMC**

The CMMC is the most widely anticipated contractor-focused cybersecurity regime since 2013 when DoD promulgated the current version of DFARS 252.204-7012. The Interim Rule follows the DoD's final CMMC. In sum, the CMMC comprises security policies and controls that are divided across five "Maturity Levels." Maturity Level 1 aligns with the 15 controls reflected in FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*.

Maturity Level 2 is an intermediary Maturity Level that is intended to help contractors moved from Maturity Level 1 to Maturity Level 3, which is required for contractor information systems that will store, transmit, or process CUI.[35]

To achieve Maturity Level 3, contractors must implement all 110 NIST SP 800-171 security controls as well as 23 additional CMMC practices and

---

[30] DFARS 204.7303(b) (Interim Rule at 61520).

[31] *Id.*; *see also* DFARS 217.207(c)(2)(i) (Interim Rule at 61520); DFARS 252.204-7019(c) (Interim Rule at 61520-21).

[32] DFARS 252.204-7019(c)(2)(i) (Interim Rule at 61520); DFARS 252.204-7019(c)(2) (Interim Rule at 61521).

[33] DFARS 252.204-7020(g)(1) (Interim Rule at 61522).

[34] DFARS 252.204-7020(g)(2) (Interim Rule at 61522).

[35] DoD does not anticipate requiring offerors/contractors to be certified at CMMC Maturity Level 2, meaning CMMC Maturity Level 2 certifications are largely irrelevant. Interim Rule at 61516.

processes. Maturity Levels 4 and 5 implemented additional, more sophisticated cybersecurity requirements intended to combat advanced persistent threats ("APTs").

Unlike the current DFARS 252.204-7012 self-certification system and, under most circumstances, the Assessment incorporated into DFARS 252.204-7019 and -7020, defense contractors subject to the CMMC will be required to undergo formal assessments "conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs)."[36] Contractors cannot rely upon POAs to demonstrate compliance, meaning companies must have implemented the applicable security requirements to be certified as compliant.[37] If the company successfully completes the assessment, a CMMC Accreditation Body ("AB") will issue a certification evidencing that the company has implemented the applicable cybersecurity controls.[38]

As with the NIST SP 800-171 Assessment Methodology, companies must hold an active CMMC certification for the requisite Maturity Level prior to award or prior to the Government exercising a contract option period where the solicitation or contract incorporates DFARS 252.204-7020.[39] To be current, a CMMC certification cannot be older than three years.[40]

Prime contractors and higher-tier subcontractors must also incorporate DFARS 252.204-7020 into lower-tier subcontracts other than those for COTS items.[41] Before awarding any subcontract, the prime contractor or higher tier subcontractor must verify that the subcontractor holds a current CMMC certification for the appropriate Maturity Level, which will depend on the nature of the information provided to the subcontractor.

## KEY TAKEAWAYS AND OUTSTANDING QUESTIONS

The NIST SP 800-171 Assessment Methodology and the CMMC implement long-anticipated policies that will revolutionize cybersecurity requirements for defense contractors. The Interim Rule, however, still leaves critical questions unanswered and raises additional concerns.

- *Preparation and Implementation*: DoD has long suggested that it the

---

[36] Interim Rule at 61506.

[37] *Id.* at 61509 ("The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action.").

[38] *Id.* at 61506.

[39] DFARS 252.204-7021(b) (Interim Rule at 61522).

[40] *Id.*

[41] DFARS 252.204-7021(g)(2) (Interim Rule at 61522).

CMMC will the forward-looking and that DoD will not amend existing contracts to incorporate CMMC certification requirements. The Interim Rule does not expressly address this issue and, as noted above, appears to leave open the possibility that DoD can amend existing contracts. Contractors that hold long-term indefinite-delivery, indefinite-quantity ("IDIQ") contracts, blanket purchase agreements ("BPAs"), and Federal Supply Schedule ("FSS") contracts under which DoD may place orders should expect DoD to incorporate the NIST SP 800-171 Assessment Methodology and CMMC requirements into task or delivery order solicitations.

- *Application of NIST SP 800-171 Assessment Methodology*: The Interim Rule does not explain how summary scores under the NIST SP 800-171 Assessment Methodology will factor into procurement decisions and contract actions. DFARS 252.204-7019 and -20 require an offeror/contractor to have a current summary score in the SPRS as the time of award or applicable contract action (e.g., exercise of an option period). However, it seems unlikely that simply having a summary score in the SPRS—which could range from 0-110—would be sufficient. DoD contracting officers would presumably consider those scores and the associated confidence levels when making award decisions and taking relevant contract actions. Yet the Interim Rule provides no guidance on this point, leaving offerors/contractors in the dark when it comes to understanding how those scores will impact their business interests.
- *Cost Allowability*: DoD has previously suggested in its CMMC Frequently Asked Questions ("FAQs") that costs associated with the CMMC certification process would be allowable.[42] The Interim Rule is silent on cost allowability and does not modify or reference existing cost principles. Thus, it remains unclear whether DoD will formally deem such costs allowable, rather than forcing contractors to rely upon nonbinding guidance in the FAQs. DoD also has not formally clarified whether contractors can recover costs associated with becoming CMMC compliant or whether contractors' recoveries will be limited to the costs of the certification process.
- *Duplicative Requirements*: The Interim Rule suggests that neither the Assessment nor the CMMC will be duplicative of each other or other DoD assessments "except for rare circumstances when a re-assessment

[42] CMMC FAQs at Question 18, https://www.acq.osd.mil/cmmc/faq.html (last visited Oct. 1, 2019).

may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance."[43] Notwithstanding these statements, the Interim Rule provides little assurance that contractors will not be required to undergo duplicative assessments. Envision a defense contractor that operates an information system that stores, processes, or transmits CUI. That contractor must comply with DFARS 252.204-7012, which requires the contractor to implement the security controls in NIST SP 800-171. That contract would also presumably incorporate DFARS 252.204-7019 and DFARS 252.204-7020, mandating that the contractor undergo an assessment in accordance with the NIST SP 800-171 Assessment Methodology. That contract would also incorporate DFARS 252.204-7021, requiring the contractor to be certified at CMMC Maturity Level 3.

If DoD truly intends to avoid duplication, then the CMMC Maturity Level 3 certification requirement would render superfluous and irrelevant any need for an assessment under DFARS 252.204-7019 or DFARS 252.204-7020. The Interim Rule, however, does not contemplate that having an existing CMMC Maturity Level 3 certification will obviate the need for a separate assessment under the NIST SP 800-171 Assessment Methodology. DoD also has not created a formal system for reciprocity between the CMMC and other programs, such as FedRAMP.

- *Procurement Eligibility and Bid Protest Risks*: Notwithstanding the concerns noted above about how contracting officers will account for NIST SP 800-171 Assessment Methodology summary scores and confidence levels in award decisions and contract actions, the Interim Rule raises significant questions about how the NIST SP 800-171 Assessment Methodology and the CMMC will impact procurement decisions. Will agencies assess compliance on pass/fail and non-comparative basis and thus essentially as a matter of responsibility,[44] or will agencies perform a comparative analysis in which they consider differences between offerors' summary scores and confidence levels? Given this uncertainty, companies would be well-advised to implement applicable security controls to the maximum extent practicable to best position themselves to compete with other offerors.

---

[43] Interim Rule at 61505, 61509.

[44] *See, e.g.*, *Lawson Envt'l Servs. LLC*, B-416892, B-416892.2, Jan. 8, 2019, 2019 CPD ¶ 17 (explaining that issues evaluated on a noncomparative basis are considered matters of responsibility).