AN A.S. PRATT PUBLICATION
NOVEMBER 2019
VOL. 5 • NO. 11

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 5 **NUMBER 11** **November 2019**

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

(2019–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. For subscription information and customer service, call 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 government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

DoD Releases Public Draft of Cybersecurity Maturity Model Certification

By Susan B. Cassidy, Samantha L. Clark, Ryan Burnette, and Ian Brekke[*]

The Office of the Assistant Secretary of Defense for Acquisition recently released Version 0.4 of its draft Cybersecurity Maturity Model Certification. The authors of this article provide an overview of the current framework draft and discuss open questions and issues for contractors.

The Office of the Assistant Secretary of Defense for Acquisition has released Version 0.4 of its draft Cybersecurity Maturity Model Certification ("CMMC") for public comment. The CMMC was created in response to growing concerns by Congress and within Department of Defense ("DoD") over the increased presence of cyber threats and intrusions aimed at the Defense Industrial Base ("DIB") and its supply chains. In its overview briefing[1] for the new model, DoD describes the draft CMMC framework[2] as a "unified cybersecurity standard" for DoD acquisitions that is intended to build upon existing regulations, policy, and memoranda by adding a verification component to cybersecurity protections for safeguarding Controlled Unclassified Information ("CUI") within the DIB. The model describes the requirements that contractors must meet to qualify for certain maturity certifications, ranging from Level 1 ("Basic Cyber Hygiene" practices and "Performed" processes) through Level 5 ("Advanced / Progressive" practices and "Optimized" processes), with such certification determinations to generally be made by third party auditors.

The CMMC establishes a new framework for defense contractors to become certified as cybersecurity compliant. DoD has stated that it intends to release Version 1.0 of the CMMC framework in January 2020 and will begin using that version in new DoD solicitations starting in Fall 2020. Notwithstanding the pendency of these deadlines, a large number of questions remain outstanding.

OVERVIEW OF THE CURRENT CMMC FRAMEWORK DRAFT

At its core, the current version of the CMMC framework consists of a matrix, composed of "Domains," "Capabilities," and "Practices and Processes." Do-

---

[*] Susan B. Cassidy (scassidy@cov.com) is a partner at Covington & Burling LLP advising clients on the rules and regulations imposed on government contractors, with a special emphasis on the defense and intelligence sectors. Samantha L. Clark (sclark@cov.com) is special counsel at the firm practicing in the Public Policy Practice Group as well as the CFIUS and Government Contracts groups. Ryan Burnette (rburnette@cov.com) and Ian Brekke (ibrekke@cov.com) are associates at the firm advising clients on a range of issues related to government contracting.

[1] https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf.

[2] https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf.

mains are comprised of Capabilities, and Capabilities are comprised of Practices and Processes. The model contains 18 different Domains of "key sets of capabilities for cybersecurity," 14 of which use the same terminology as the security requirement families in NIST Special Publication (SP) 800-171. The model adds Asset Management, Cybersecurity Governance, Recovery, and Situational Awareness to the NIST SP 800-171 security requirement families. The 18 Domains are:

- Access Control
- Asset Management*
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Cybersecurity Governance*
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Recovery*
- Risk Assessment
- Security Assessment
- Situational Awareness*
- System and Communications Protection
- System and Information Integrity

(*Domain is not one of the 14 NIST SP 800-171 security requirement families.)

Each Domain lists certain Capabilities, which are "achievements to ensure cybersecurity within each domain." In total, to achieve the highest level of certification—Level 5—contractors must comply with more than 80 different individual Capabilities, such as the ability to "detect and report events" and the ability to "implement threat monitoring based on defined requirements."

Capabilities are comprised of much more detailed "Practices" and "Processes" that contractors must adhere to. Practices are similar to security controls, and

DoD has described them as "activities required by level to achieve a capability." Processes, by contrast, are intended to detail the maturity of the institutionalization of the practices.

Although the NIST SP 800-171 controls are referenced in the model (and "coverage" of all NIST SP 800-171 rev 1 security controls is a requisite for meeting Level 3 certification), many of the practices have been informed by other sources, such as ISO 27001:2013, AIA NAS 9933, and the CERT Resilience Management Model, in addition to best practices gathered from DIB members. Many of requirements, particularly for Level 5 certification, would be new for contractors, and cite to DIB best practices as a source. Noticeably absent are citations to NIST SP 800-171B, which NIST published in draft form in June 2019 with enhanced security requirements designed to protect designated "high value assets" or "critical programs" that contain CUI of interest to advanced persistent threats. Accordingly, there remain questions about how these controls should be interpreted and whether additional guidance for implementation will accompany future versions of the model.

Unlike NIST SP 800-171, which is implemented through a regulation—*i.e.*, DFARS clause 252.204-7012—DoD plans to implement the requirements of the model on a purely contractual basis. The required CMMC level applicable to a procurement will be listed in the solicitation in sections L and M and will be a "go/no-go decision."

DoD has stated that the model is still being refined, that practices within the model have not yet been cross-referenced across Domains, and that it anticipates a reduction in size of the model as it is further developed. DoD indicated in the overview briefing accompanying the model that it intends to use independent third party organizations to conduct audits and certify contractors. DoD has released neither the methodology to handle maturity level trade-offs, nor the assessment guidance for these third-party certifiers. Nonetheless, as stated above, DoD plans to have a final version of the CMMC framework released in January 2020, included in RFIs starting in June 2020, and included in RFPs starting in Fall 2020.

OPEN QUESTIONS AND ISSUES FOR CONTRACTORS

The draft CMMC framework provides significant information about the specific requirements that DoD may impose on contractors seeking certain certification thresholds, but leaves open many important questions for contractors.

- *Implementation Deadlines.* The CMMC introduces a significant number of new controls and requirements. Even the most sophisticated of contractors will likely find compliance difficult and the continued maturation of the model will make compliance with DoD's ambitious

deadlines a challenge across the DIB.

- *Determination of Appropriate CMMC Level for Contracts*. The guidance offers no insight into how DoD will determine the CMMC certification level required for each contract solicitation or whether it intends to standardize a process for making such determinations across the Departments or even within requiring activities. Existing FAQs[3] on DoD's CMMC website only state that "[t]he government will determine the appropriate tier (i.e. not everything requires the highest level) for the contracts they administer."
- *Allowable Costs.* DoD has consistently said that the costs of compliance with the CMMC would be allowable. Presumably these costs would be recovered in contractors' overhead rates. However, to the extent that commercial item contractors—including many small business—contract with the government on a price basis, the costs of implementation would not be separately reimbursable by the government.
- *Meeting a Certification Level.* The CMMC framework does not provide guidance on how each of the Capabilities within the various Domains are to be weighed against one another, and similarly, how compliance with each of the respective Practices within Capabilities are to be weighed against one another. It is unclear, for example, whether compliance with each Practice or Capability will be given equal weight, whether DoD will assign some relative level of importance to each Practice or Capability, or whether this will be largely left to the discretion of the auditor. Although DoD has stated that "[a] methodology to handle maturity level trade-offs is planned" and that "[d]etailed assessment guidance is still under development," it is not apparent whether the forthcoming guidance will address any of these points. Nor is it clear the extent to which prior guidance on Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented (*i.e.*, Impact Guidance) may apply to the model.
- *Audit Determinations.* It is not clear what recourse, if any, contractors might have to challenge a CMMC certification determination by an auditor. Although DoD has stated that "[s]ome of the higher level assessments may be performed by organic DoD assessors within the Services, the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA)," for lower-

[3] https://www.acq.osd.mil/cmmc/faq.html.

level assessments, auditors appear to be vested with a great deal of discretion. For example, DoD recognized "the challenges of being 100% compliant with some practices," and suggested that an "[a]ssessment of process institutionalization helps to mitigate this concern." However, it is not clear how auditors are expected to balance overall compliance with Practices against efforts that contractors have taken towards process institutionalization (*e.g.*, Procedures).

- *Subcontractor Compliance Requirements.* DoD has not yet issued any guidance on the certification level required for subcontractors, including whether the prime contractor is responsible for making this determination or if all subcontractors must meet the level assigned to a particular contract regardless of the data that flows to those subcontractors.
- *Implementation by Policy vs. Regulation.* Ordinarily, we would expect these types of requirements for DoD contracts to be addressed through the regulatory process. Making the change through policy allows DoD to implement the requirements more quickly, but does leave open the possibility of divergence among the Departments such as what the DIB has seen over the past year with the unique cybersecurity requirements being issued by the Navy and other Departments.
- *Protest Considerations.* It is not clear whether contractors will have any ability to appeal or successfully protest the CMMC level at which DoD has designated a contract, and if so, whether this will be the only mechanism available to contractors to ensure that agencies give second thought to a particular CMMC level. For example, in the pre-award context, prospective offerors may consider protesting the level assigned to a particular procurement as overly restrictive of competition. Although deference is usually provided to agencies in the area of national security, the viability and success of this and other protest grounds remains to be seen.