AN A.S. PRATT PUBLICATION
JANUARY 2020
VOL. 6 • NO. 1

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

EDITOR'S NOTE: CERTIFICATION
Victoria Prussen Spears

DOD'S DRAFT CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK
Charles A. Blanchard, Ronald D. Lee, Sonia Tabriz, and Amanda J. Sherwood

DEPARTMENT OF JUSTICE ISSUES NEW GUIDANCE ON EXEMPTION 4 TO THE FREEDOM OF INFORMATION ACT
Alex D. Tomaszczuk, John E. Jensen, and Aaron S. Ralph

CISA INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE ISSUES NEW INTERIM REPORT
Susan B. Cassidy and Ryan Burnette

LOWEST PRICED TECHNICALLY ACCEPTABLE PROCUREMENTS NOT ALWAYS ACCEPTABLE: NEW DFARS RULE CONTINUES SHAKE-UP OF LPTA PROCUREMENTS
Kayleigh Scalzo and Andrew Guy

IN THE COURTS
Steven A. Meyerowitz

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 6 **NUMBER 1** **January 2020**

Editor's Note: Certification
Victoria Prussen Spears 1

DoD's Draft Cybersecurity Maturity Model Certification Framework
Charles A. Blanchard, Ronald D. Lee, Sonia Tabriz, and Amanda J. Sherwood 3

Department of Justice Issues New Guidance on Exemption 4 to the Freedom of Information Act
Alex D. Tomaszczuk, John E. Jensen, and Aaron S. Ralph 12

CISA Information and Communications Technology Supply Chain Risk Management Task Force Issues New Interim Report
Susan B. Cassidy and Ryan Burnette 15

Lowest Priced Technically Acceptable Procurements Not Always Acceptable: New DFARS Rule Continues Shake-Up of LPTA Procurements
Kayleigh Scalzo and Andrew Guy 19

In the Courts
Steven A. Meyerowitz 23

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.

An A.S. Pratt® Publication
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 twelve times a year by Matthew Bender & Company, Inc. 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. 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, 630 Central Avenue, New Providence, NJ 07974.

DoD's Draft Cybersecurity Maturity Model Certification Framework

By Charles A. Blanchard, Ronald D. Lee, Sonia Tabriz, and Amanda J. Sherwood*

The Department of Defense has taken another step towards definitizing the cybersecurity requirements applicable to all of its contractors beginning in 2020, in the form of Cybersecurity Maturity Model Certification. The authors of this article discuss the Model Certification.

The Department of Defense ("DoD") has taken another step towards definitizing the cybersecurity requirements applicable to all of its contractors beginning in 2020, in the form of Cybersecurity Maturity Model Certification ("CMMC"). The CMMC could be a positive step towards developing a unified standard for defense contractor cybersecurity, but it is critical that industry stakeholders provide substantive feedback on the various practices and processes the current draft proposes to ensure they are practicable, likely to produce the desired effects, and clearly articulate DoD's expectations.

Furthermore, the benefit to contractors of such a unified standard will be necessarily bounded unless and until the civilian agencies undertake a similar effort to streamline cybersecurity requirements.

BACKGROUND

As defense contractors are well aware, cybersecurity requirements applicable to defense procurements have long been an important issue. DFARS 252.204-7012, which went into effect on December 31, 2017, generally requires that defense contractors comply with the National Institute of Standards and Technology's Special Publication 800-171 ("NIST SP 800-171") in "safeguarding" enumerated defense information and reporting cybersecurity incidents. But, it has become increasingly clear that not only is compliance with NIST SP

* Charles A. Blanchard (charles.blanchard@arnoldporter.com), a partner at Arnold & Porter Kaye Scholer LLP, works with clients in the contracting and national security communities, providing unique insights into doing business with the federal government. 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. Sonia Tabriz (sonia.tabriz@arnoldporter.com) is an associate at the firm advising clients regulated by and performing work for the federal government across a variety of industries. Amanda J. Sherwood (amanda.sherwood@arnoldporter.com) is an associate at the firm focusing on a wide range of government contracts matters. Trevor Schmitt, a graduate of Georgetown University Law Center, employed at the firm, but not admitted to the practice of law in Washington, D.C., contributed to this article.

800-171 complex, but reliance on NIST standards alone may not prevent high-profile security incidents, let alone provide DoD with a readout on the cybersecurity maturity of its defense industrial base.

The multiplicity of available standards—applied to varying degrees by different federal agencies—has also long frustrated industry. Challenges with delineating which standards apply and how to comply with each confound even the most experienced contractors, and may serve as a barrier to entry for small businesses and other companies entering the federal marketplace for the first time.

To resolve these concerns, last year DoD announced the development of the CMMC, which aims to "assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB)"[1] by "reduc[ing] exfiltration of Controlled Unclassified Information (CUI)."[2] The CMMC will combine the existing alphabet soup of security standards—including NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933—into a unified standard for defense contractor cybersecurity.[3]

DoD has stated that "[u]nlike NIST SP 800-171, CMMC will implement multiple levels of cybersecurity" and "[i]n addition to assessing the maturity of a company's implementation of cybersecurity controls, the CMMC will also assess the company's maturity/institutionalization of cybersecurity practices and processes."[4] Notably, the CMMC will build upon these existing regulations and standards by adding a verification component to identified cybersecurity practices.[5]

CMMC will not be a self-certification; instead, all companies doing business with DoD, including subcontractors, must be certified by an independent third party commercial certification organization.[6] The framework will permit

---

[1] Office of the Under Sec'y of Def. of Acquisition & Sustainment, Cybersec. Maturity Model Certification, CMMC Frequently Asked Questions (FAQ's), Question 5, https://www.acq.osd.mil/cmmc/faq.html.

[2] Office of the Under Sec'y of Def. of Acquisition & Sustainment, Draft CMMC Model Rev 0.4 Release & Request for Feedback Overview 4 (Sept. 2019) (hereinafter "CMMC Rev 0.4 Overview"), https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf.

[3] CMMC Frequently Asked Questions (FAQ's), *supra* note 1, at Question 8.

[4] CMMC Frequently Asked Questions (FAQ's), *supra* note 1, at Question 9.

[5] CMMC Rev 0.4 Overview, *supra* note 2, at 5.

[6] *See* CMMC Frequently Asked Questions (FAQ's), *supra* note 1, at Questions 12–14. In the case of "higher level assessments," the certification will be performed by "DoD assessors within the Services, the Defense Contract Management Agency (DMCA) or the Defense Counterintelligence and Security Agency (DCSA)." CMMC Frequently Asked Questions

contractors to certify several increasing levels of cybersecurity (from "Basic Cybersecurity Hygiene" to "Advanced"), with the intent that the lowest level will be relatively inexpensive and broadly accessible to even the smallest contractors.[7] DoD has announced that the costs of obtaining the certification will be considered an allowable, reimbursable cost and "will not be prohibitive."[8]

DRAFT CMMC VERSION 0.4

The CMMC framework remains a work in progress. DoD indicated that it plans to publish Version 1.0 of the CMMC in January 2020, so that the certification requirement can be incorporated into Requests for Information in June 2020 and used as a "go/no go" evaluation factor in Requests for Proposals beginning in Fall 2020.[9]

DoD recently took one of many steps to reach that end goal. On September 4, 2019, DoD released an early version of the CMMC, which it calls the "Draft CMMC Version 0.4."[10] In this document, which DoD has characterized as the "midpoint" of CMMC development,[11] the CMMC framework is comprised of three main elements: (1) domains; (2) capabilities within each domain; and (3) practices and processes.

(FAQ's), *supra* note 1, at Question 14 (DOD has not defined what these "higher level assessments" may be).

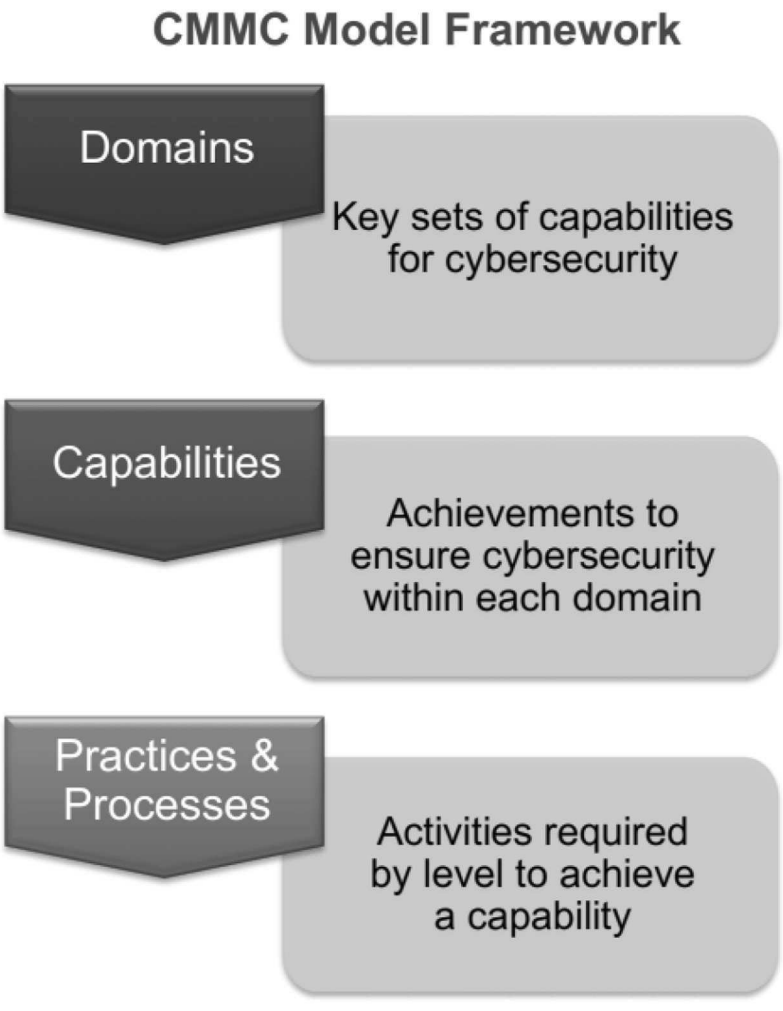
[7] *Id.* at Question 4.

[8] *Id.* at Question 19; *see also* CMMC Rev 0.4 Overview, *supra* note 2, at 5 ("The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.").

[9] CMMC Rev 0.4 Overview, *supra* note 2, at 4.

[10] Office of the Under Sec'y of Def. of Acquisition & Sustainment, Draft CMMC Model Version 0.4 (Aug. 30, 2019), https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf.

[11] Office of the Under Sec'y of Def. of Acquisition & Sustainment, Cybersec. Maturity Model Certification, Draft CMMC v0.4, https://www.acq.osd.mil/cmmc/draft.html.



The first element of the CMMC framework is 18 cybersecurity domains, which reflect what DoD considers to be "[k]ey sets of capabilities for cybersecurity." These domains include:

- Asset 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; and
- Systems and Information Integrity.[12]

These domains are, in turn, comprised of various cybersecurity capabilities, i.e., "[a]chievements to ensure cybersecurity within each domain," which are further divided into individual practices and processes for each domain.[13] The CMMC calls on contractors and certifiers to consider whether the company's practices and procedures are designed to ensure cybersecurity. Practices are defined cybersecurity activities, whereas processes "detail maturity of institutionalization for the practices."[14]

Importantly, the duality of practices and processes reflects DoD's recognition of industry feedback regarding the challenges of achieving 100 percent compliance with certain practices. By assessing the contractor's institutionalization of processes intended to manage the environment in which CUI resides, DoD will be assured that practices are being implemented effectively.[15]

The practices and processes are then mapped to five cumulative maturity levels. For each CMMC level, the associated practices and processes aim to reduce risks for a specific set of cyber threats. Levels 1 through 5 range from cost effective and affordable practices achievable for small businesses through highly advanced practices required for the most critical DoD systems.[16] The corresponding processes in each level reflect the degree of optimization achieved by the contractor.

---

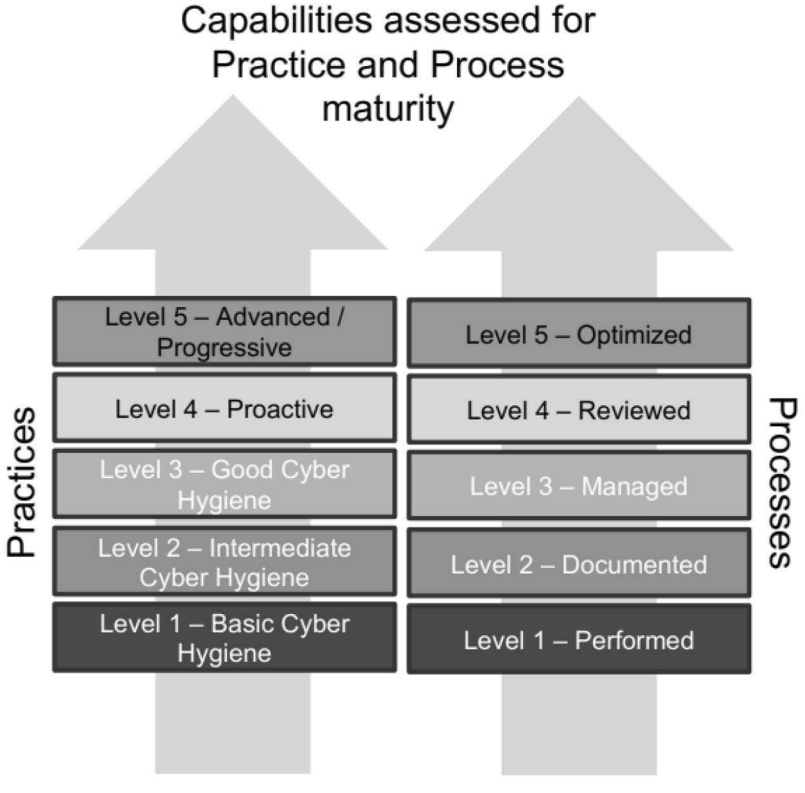
[12] CMMC Rev 0.4 Overview, *supra* note 2, at 8, 10.

[13] *Id.* at 8.

[14] *Id.*

[15] *See id.* at 11.

[16] *See id.* at 9–10.



The particular requirements under each level vary. For instance, under Level 1 (Basic Cyber Hygiene), a contractor must only comply with the FAR requirements and implement ad hoc incident response and cybersecurity governance. The NIST SP 800-171 requirements—previously many contractors' key cybersecurity compliance concern—only appears in Level 3 (Good Cyber Hygiene), which also requires that the contractor maintain an Information Security Continuity Plan and communicate threat information to key stakeholders. And, NIST SP 800-171 is not considered the "gold standard" of cybersecurity compliance—two additional levels exist beyond it. Under Levels 4 and 5, contractors must implement additional safeguards, such as threat hunting, network segmentation, real-time asset tracking, 24x7 SOC operation, device authentication, and autonomous initial response actions.[17]

---

[17] *Id.* at 16. According to DoD, Levels 4 and 5 are "targeted toward a small subset of the DIB sector that supports DOD critical programs and technology," and therefore will not apply to large swaths of defense contractors. *Id.*

These are just examples of the practices that apply by level but demonstrate the tiered approach—an approach under which DoD believes all contractors in its supply chain can achieve some level of compliance. DoD will assess and identify the appropriate CMMC level for a particular contract and incorporate that level into the solicitation, thereby designating the pool of defense contractors eligible to compete.[18]

In a presentation accompanying the Draft CMMC Version 0.4, DoD explained that between now and issuance of the finalized Version 1.0 in January 2020, it intends to both refine and reduce the size of the CMMC, to include options for "[d]own selecting, prioritizing and consolidating capabilities."[19] DoD also intends to incorporate a "methodology to handle maturity level trade-offs."[20] DoD also requested feedback from industry stakeholders, including responses to questions regarding:

(1) Recommendations to remove or de-prioritize certain requirements to simplify the model;

(2) Elements that provide high value to the organization;

(3) Whether any practices should be moved or cross-referenced between levels or domains; and

(4) Recommendations to clarify any practices or processes.[21]

KEY TAKEAWAYS

The impact of the CMMC cannot be overstated. This long-awaited framework of cybersecurity requirements will apply to all contractors doing business with DoD, including subcontractors. Although the required practices and processes may vary based upon the cybersecurity risks at issue, every defense contractor will be required to achieve the requisite certification in order to receive the "go" rating necessary to be considered for award. Open questions remain as to the practical and legal implications of this process:

- While DoD is emphatic that the CMMC will apply to all contractors and subcontractors, as always, the devil lies in the details. How many levels of subcontractors down will certifications apply? Especially given DoD's recent focus on supply chain integrity, industry should be prepared for certifications to apply beyond the first tier of subcontracting. If so, where will the responsibility lie—with the prime contractor, or

---

[18] *See* CMMC Frequently Asked Questions (FAQ's), *supra* note 1, at Question 4.

[19] CMMC Rev 0.4 Overview, *supra* note 2, at 6.

[20] *Id.*

[21] *Id.* at 18; Draft CMMC v0.4, *supra* note 11.

will DoD assert regulatory power over every supplier no matter how distant?

- If DoD determines that subcontractor(s) require a lower level of certification than the prime, then will DoD accordingly limit the contract-related information that can be shared with the subcontractor(s)? Will DoD constrain or prohibit connectivity of information systems between the prime and lower level subcontractor(s)?
- What about commercial item contracts? Small businesses?
- The whole framework relies on a network of independent certifiers—who will certify the certifiers? Who will be responsible for their mistakes and oversights? And as a practical matter, will enough certifiers be available to certify the entire defense contracting industry when CMMC "goes live?" Will there be a backlog of certifications, and if so how will DoD handle variance requests?
- DoD contractors have made significant investments in complying with the existing framework—including NIST SP 800-171. Will DoD allow for a transition period to the new certification requirements for option years or new task orders under existing contracts?
- Will certification offer any protection from potential False Claims Act allegations resulting from an alleged noncompliance?
- There will be an incentive for DoD to require a higher CMMC level than necessary in solicitations—will that be protestable, or must industry concede to DoD judgment regarding the necessary level of cybersecurity protection in the national defense space?

The good news is that costs for obtaining the requisite certification will be considered allowable, and DoD appears to recognize that 100 percent compliance with certain practices (especially in complex or exceptionally large IT environments) is impracticable. Nevertheless, it remains critical that industry stakeholders submit feedback regarding Version 0.4 of the CMMC to gain insights on the above and other open questions as well as to help frame the substantive security requirements by level as DoD barrels towards finalization of Version 1.0 in January 2020.

It is also ever important that civilian agencies follow suit. The patchwork of cybersecurity requirements that currently govern federal contractors performing work for both civilian and defense agencies renders it costly and challenging to remain compliant, despite best efforts. Civilian agencies should strongly consider collaborating with DoD to adopt the same framework and certification requirements rather than developing a parallel set of practices and

processes, which will yield further ambiguity both for longstanding contractors and those seeking to enter the federal marketplace.