AN A.S. PRATT PUBLICATION
JULY 2020
VOL. 6 • NO. 7

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis

EDITOR'S NOTE: THE CARES ACT
Victoria Prussen Spears

CERTIFIER BEWARE: CERTIFICATIONS AND LIABILITY UNDER THE FALSE CLAIMS ACT
James M. Davis, Robert G. Tweel, and Alaina N. Crislip

CARES ACT INCLUDES ASSISTANCE TO FEDERAL CONTRACTORS WHO OFFER EMPLOYEES PAID LEAVE
Kevin J. Cosgrove and Lawrence K. DeMeo

THE CARES ACT AND MITIGATING FALSE CLAIMS ACT RISK
Breon S. Peace, Jennifer Kennedy Park, Jonathan S. Kolodner, Lisa Vicens, and Charity E. Lee

SELLERS BEWARE: THE BLURRY LINE BETWEEN PROFIT AND PRICE GOUGING UNDER THE DEFENSE PRODUCTION ACT
Carolina A. Fornos, Mark R. Hellerer, and Colin Davis

DOD CYBERSECURITY MATURITY MODEL CERTIFICATION IMPOSES AUDIT AND ACCREDITATION PROCESSES TO VERIFY COMPLIANCE WITH COMPREHENSIVE CYBERSECURITY REQUIREMENTS
Charles A. Blanchard, Ronald D. Lee, Nicholas L. Townsend, Tom McSorley, Sonia Tabriz, Amanda J. Sherwood, and Thomas Pettit

THE DATA RIGHTS BLACK HOLE: DOD LOBBIES CONGRESS TO ELIMINATE PROPRIETARY RIGHTS IN YOUR MOST VALUABLE TRADE SECRETS – YOUR DETAILED MANUFACTURING AND PROCESS DATA
W. Jay DeVecchio

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 6 | NUMBER 7 | July 2020

Editor's Note: The CARES Act
Victoria Prussen Spears 221

Certifier Beware: Certifications and Liability Under the False Claims Act
James M. Davis, Robert G. Tweel, and Alaina N. Crislip 223

CARES Act Includes Assistance to Federal Contractors Who Offer Employees Paid Leave
Kevin J. Cosgrove and Lawrence K. DeMeo 230

The CARES Act and Mitigating False Claims Act Risk
Breon S. Peace, Jennifer Kennedy Park, Jonathan S. Kolodner, Lisa Vicens, and Charity E. Lee 235

Sellers Beware: The Blurry Line Between Profit and Price Gouging Under the Defense Production Act
Carolina A. Fornos, Mark R. Hellerer, and Colin Davis 239

DoD Cybersecurity Maturity Model Certification Imposes Audit and Accreditation Processes to Verify Compliance with Comprehensive Cybersecurity Requirements
Charles A. Blanchard, Ronald D. Lee, Nicholas L. Townsend, Tom McSorley, Sonia Tabriz, Amanda J. Sherwood, and Thomas Pettit 244

The Data Rights Black Hole: DoD Lobbies Congress to Eliminate Proprietary Rights in Your Most Valuable Trade Secrets – Your Detailed Manufacturing and Process Data
W. Jay DeVecchio 254

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.

DoD Cybersecurity Maturity Model Certification Imposes Audit and Accreditation Processes to Verify Compliance with Comprehensive Cybersecurity Requirements

By Charles A. Blanchard, Ronald D. Lee, Nicholas L. Townsend, Tom McSorley, Sonia Tabriz, Amanda J. Sherwood, and Thomas Pettit*

This article provides background about the Cybersecurity Maturity Model Certification, describes its structure and principal features, and discusses implementation.

The Department of Defense ("DoD") issued its long-awaited final Cybersecurity Maturity Model Certification ("CMMC"),[1] which DoD hopes will combat the immense toll cyber threats have taken on the Defense Industrial Base ("DIB"), the U.S. economy, and national security.[2] The final CMMC provides a comprehensive framework of cybersecurity controls and policies that defense contractors must implement depending on the nature of the information that their information systems will process, store, or transmit. This article provides background about the CMMC, describe its structure and principal features, and discuss implementation. While this is a DoD-specific effort that does not apply to other agencies, DoD is working with civilian agencies, including the Department of Homeland Security Cybersecurity and Infrastructure Security Agency with the goal of making this a government-wide program.[3]

The CMMC and associated DoD guidance suggest that DoD intends to implement the CMMC through procurement-specific solicitation provisions

---

* Charles A. Blanchard (charles.blanchard@arnoldporter.com), Ronald D. Lee (ronald.lee@arnoldporter.com), Nicholas L. Townsend (nicholas.townsend@arnoldporter.com), Tom McSorley (tom.mcsorley@arnoldporter.com), Sonia Tabriz (sonia.tabriz@arnoldporter.com), Amanda J. Sherwood (amanda.sherwood@arnoldporter.com), and Thomas Pettit (thomas.pettit@arnoldporter.com) are attorneys at Arnold & Porter Kaye Scholer LLP.

[1] CMMC Model v1.0 Briefing, https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf; CMMC Model v1.0 https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf; CMMC Model v1.0 Appendices, https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf.

[2] DoD noted that "[t]he Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016." CMMC Model v1.0, *supra* n.1, at 1.

[3] Jackson Barnett, FedScoop (Apr. 16, 2020), https://www.fedscoop.com/cmmc-federal-standards-for-acqusition/.

rather than by issuing new Defense Federal Acquisition Regulation Supplement ("DFARS") clauses or revising existing DFARS clauses, such as DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." However, as discussed below, the CMMC will materially change what defense contractors must do to safeguard information and will in some respects override aspects of the DFARS 252.204-7012 regime (e.g., eliminating the self-assessment system). As the CMMC is phased in, defense contractors must continue to ensure that they comply with all DFARS 252.204-7012 requirements, which remain relevant for nearly all defense contracts and contractors.

It is unclear whether and how the novel coronavirus ("COVID-19") will impact DoD's planned rollout of the CMMC. In March 2020, Katie Arrington, DoD's Chief Information Security Officer for Acquisition, suggested that COVID-19 would not delay implementation of the CMMC.[4] Circumstances on the ground have certainly changed since March, with all but eight states issuing some form of stay-at-home order that, as a practical matter, will impede the abilities of DoD to train and deploy accreditors and companies to access to develop information technology ("IT") and cybersecurity infrastructure necessary to implement the CMMC. However, contractors that want to be well-positioned to compete for government contracts subject to the CMMC and that want to have an advantage over their competitors should heed DoD's warning that it will do its best to stay on track by taking the steps necessary to implement the standards reflected in the CMMC.

BACKGROUND

DoD's release of the CMMC is its latest effort to expand cybersecurity requirements to contractors and their supply chains. The modern government cybersecurity system began in earnest in 1988 when Congress enacted the Computer Security Act ("CSA"), which required the National Bureau of Standards – now the National Institute for Standards and Technology ("NIST") – to create guidelines for securing government information systems.[5] In 2002, Congress replaced the CSA with the Federal Information Security Modernization Act (amended through the Federal Information Security Modernization Act of 2014 ("FISMA")). FISMA requires agencies to, among other things, (1) comply with information security standards developed and implemented in most instances by the Office of Management and Budget ("OMB") and NIST

---

[4] Mariam Baksh, Nextgov (Mar. 26, 2020), https://www.nextgov.com/cybersecurity/2020/03/coronavirus-will-not-delay-pentagons-contractor-cybersecurity-program-official-says/164152/.

[5] Computer Security Act of 1987, Pub. L. No. 100-235 (Jan. 8, 1988).

and (2) develop information security programs, which must include periodic risk assessments to test vulnerabilities and potential impacts of unauthorized intrusions.[6]

Although FISMA requires agencies to apply cybersecurity standards to "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency,"[7] there has been substantial uncertainty about how these standards apply to contractors and whether and how contractors must incorporate these security standards into their supply chains. For most federal contractors, the Federal Acquisition Regulation ("FAR") contains a limited provision at FAR Subpart 4.19 and contract clause FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems,"[8] which establish baseline security standards for any information system "owned or operated by a contractor that processes, stores, or transmits" "federal contract information" ("FCI") (i.e., "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government").

DoD contractors, however, have been subject to a broader and evolving set of standards since DoD first implemented cybersecurity standards for the defense supply chain at DFARS 252.204-7012, which has been captioned since 2015 "Safeguarding Covered Defense Information and Cyber Incident Reporting." This regulation currently applies to any "unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits" controlled unclassified information ("CUI") that qualifies as "covered defense information" ("CDI") under the rule.[9] Contractors must protect these information systems by, among other things, implementing the security controls in NIST Special Publication ("SP") 800-171r1.[10] It also directs contractors to report cyber incidents.[11] However, this system has lacked

---

[6] 44 U.S.C. § 3554.

[7] *Id.* § 3554(a)(1)(A)(ii).

[8] 81 Fed. Reg. 30439 (May 16, 2016).

[9] DFARS 252.204-7012(a). CUI is any unclassified information subject to "safeguarding or dissemination controls." 32 C.F.R. § 2002.4(h). Categories and subcategories of CUI are identified in the CUI Registry. https://www.archives.gov/cui/registry/category-list. CDI is CUI that "is (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." DFARS 252.204-7012(a).

[10] DFARS 252.204-7012(b).

[11] DFARS 252.204-7012(c).

verification and enforcement mechanisms, such as independent audits, though the risk of False Claims Act liability looms over potentially noncompliant contractors, as illustrated by the recent decision in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*

CMMC

DoD has determined that more must be done to harden the DIB's and defense supply chain's cyber infrastructure. Enter the CMMC, which DoD announced in May 2019 as a consolidated framework of cybersecurity controls and practices that will apply to contractor-owned and contractor-operated information systems that store or transmit FCI or CUI. The final CMMC follows seven drafts, with the first issued in May 2019 and the seventh issued in December 2019.

CMMC v1.0 incorporates not only the baseline requirements established in FAR 52.204-21 and the cybersecurity controls and practices provided in NIST SP 800-171r1 but also those in Draft NIST SP 800-171B and guidance from other organizations.[12] The CMMC also imposes audit and accreditation requirements to provide a mechanism for verifying and enforcing compliance. These requirements will ultimately apply to all contractors and subcontractors throughout the supply chain.[13]

---

[12] CMMC Frequently Asked Questions (FAQs), at Question 8, https://www.acq.osd.mil/cmmc/faq.html (last visited Feb. 6, 2020).

[13] *Id.* at Question 21 ("[A]ll companies doing business with the Department of Defense will need to obtain CMMC.").

CMMC STRUCTURE

DoD retained the general structure of the draft CMMC versions in the final version. CMMC v1.0 allocates cybersecurity controls and policies through a multi-level system of domains, capabilities, and practices and processes. There are 17 domains, which are categories of cybersecurity controls that build upon the 14 "families" of security controls in NIST SP 800-171:[14]

The domains are made of up capabilities.[15] These capabilities (i.e., "[a]chievements to ensure cybersecurity within each domain"[16]) are further divided into specific cybersecurity controls and policies known as practices and processes.[17] The practices and processes are allocated across five maturity levels, with Maturity Level 1 imposing baseline security requirements reflected in FAR 52.204-21 and each higher maturity level imposing more intense and sophisticated practices and processes:[18]

---

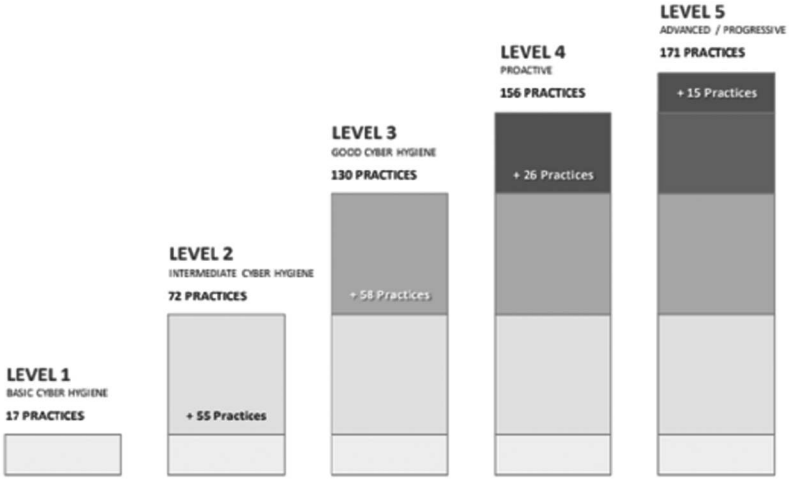
[14] *Compare* CMMC Model v1.0, *supra* n.1, at 7 with NIST SP 800-17r1 at 7, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. Through the drafting process, DoD removed the Cybersecurity Governance domain. *Compare* CMMC Draft Version 0.4 Release & Request for Feedback at 10 with CMMC Draft Version 0.6 Preface at 5 and CMMC Model v1.0, *supra* n.1, at 7.

[15] CMMC Model v1.0, *supra* n.1, at 8.

[16] CMMC Draft v0.4 Overview at 8, https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf.

[17] CMMC Model v1.0, *supra* n.1, at 7-8.

[18] *Id.* at 10, 11.



Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Maturity Level 2 will be a transition step to allow contractors to achieve Maturity Level 3, which organizations must attain to be able to process, store, or transmit CUI and which requires organizations to implement security controls in NIST SP 800-171r1.[19] Levels 4 and 5 impose more sophisticated requirements, including many controls contained in Draft NIST SP 800-171B.[20] Notably, the CMMC tests not only whether specific systems adequately implement the controls in NIST SP 800-171r1 but also the extent to which cybersecurity practices and processes are institutionalized, indicating that DoD expects organizations to secure their cyber infrastructure more broadly, and perhaps even companywide.[21]

---

[19] *Id.* at 10.

[20] *Id.* at 10-11.

[21] *Id.* at 11.

CMMC IMPLEMENTATION AND ROLL-OUT

DoD will implement and roll-out the CMMC in phases. These phases include developing assessment and certification procedures and authorities; accrediting assessors; training stakeholders, including industry, on the CMMC; and incorporating the CMMC into DoD contracts.

CMMC Assessment and Certification

DoD recognized that it needed procedures for auditing and certifying CMMC compliance. To accomplish this goal, DoD created a number of stakeholders with defined roles. The most prominent stakeholder is the CMMC Accreditation Body ("CMMC-AB"), which is a nonprofit, 501(c)(3) organization. According to DoD, which is a CMMC-AB stakeholder, half of the CMMC-AB's directors have small business backgrounds.[22] The CMMC-AB's roles and responsibilities are laid out in a memorandum of understanding ("MOU") with DoD, including "oversee[ing] the training, quality and administration of the CMMC third-party assessment organizations ("C-3PAOs") and individual assessors."[23]

C-3PAOs and individual assessors will be responsible for auditing and certifying companies' compliance with the CMMC.[24] These audits will consist of "[i]ndependent review[s] and examination[s] of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures."[25] Based on the results of those audits, C-3PAOs and individual assessors will certify an organization as having achieved the maturity level against which it was assessed.[26] To ensure independence and avoid conflicts of interest, these assessors will not be allowed to assess their own organizations.[27] The CMMC-AB has not yet established

---

[22] *Press Briefing by Under Secretary of Defense for Acquisition & Sustainment Ellen M. Lord, Assistant Secretary of Defense for Acquisition Kevin Fahey, and Chief Information Security Officer for Acquisition Katie Arrington*, DoD (Jan. 31, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/ (hereinafter "DoD Press Briefing").

[23] *Id.*

[24] DoD has suggested that assessments for the highest maturity levels "may be performed by organic DoD assessors within the Services, the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA)." CMMC FAQs, *supra* n.12, at Question 14.

[25] CMMC-AB Glossary, https://www.cmmcab.org/glossary (last visited Feb. 6, 2020).

[26] DoD Press Briefing, *supra* n.22.

[27] CMMC-AB Glossary, *supra* n.25.

procedures for accrediting C-3PAOs and individual assessors, but DoD expects the CMMC-AB to "have a marketplace on their website in March or early April of 2020, where companies can start coming in and getting information."[28]

CMMC Training

DoD is working with the Defense Acquisition University ("DAU") to develop CMMC training.[29] This training should be posted to DAU's website in or around June 2020.[30]

CMMC Implementation

DoD expects to begin implementing the CMMC and applying those requirements to contractors and their supply chains in or around March 2020. This process will begin with a "pathfinder" program. Although DoD believes it has a strong understanding of how burdensome the CMMC will be when implementing the CMMC, DoD will use pathfinders to test the CMMC process and determine "how long it is actually taking for someone to come in who's never seen the model actually run through an assessment."[31]

Contractors can expect DoD to begin incorporating the CMMC into requests for information ("RFIs") beginning in June 2020 with contract awards incorporating the CMMC starting in Fiscal Year ("FY") 2021.[32] The CMMC will initially be limited to "candidate programs."[33] It is not clear how many procurements this initial implementation will affect, but reports suggest that roughly 10 to 20 procurements may be impacted in the short-term.[34] DoD will ultimately incorporate the CMMC into every new DoD contract – including other transaction agreements ("OTAs") – starting in FY2026.[35]

---

[28] DoD Press Briefing, *supra* n.22.

[29] *Id.*

[30] *Id.*

[31] Lauren C. Williams, *A sneak peek at CMMC*, FCW (Jan. 29, 2020), https://fcw.com/articles/2020/01/29/cmmc-preview-arrington-cyber.aspx.

[32] DoD Press Briefing, *supra* n.22.

[33] *Id.*

[34] Jared Serbu, *Pentagon issues long-awaited cyber framework for Defense Industry*, Fed. News. Network (Jan. 31, 2020), https://federalnewsnetwork.com/defense-main/2020/01/pentagon-issues-long-awaited-cyber-framework-for-defense-industry/ (indicating the initial roll-out will be limited to 10 contracts); Travis J. Tritten, *Defense Contractor Cybersecurity Audits Move Closer to Reality*, Bloomberg Gov't (Jan. 31, 2020), https://news.bloomberglaw.com/tech-and-telecom-law/defense-contractor-cybersecurity-audits-move-closer-to-reality (indicating the initial roll-out will apply to 20 procurements).

[35] DoD Press Briefing, *supra* n.22.

KEY TAKEAWAYS

The CMMC is a groundbreaking new cybersecurity effort that will have vast implications for contractors as DoD implements it over the next six years and as it becomes mandatory for all DoD contractors and their supply chains. As of June 2019, only one percent of the DIB had implemented NIST SP 800-171's 100 security controls.[36] The implementation of CMMC will likely increase this number dramatically. Moving forward, contractors should bear in mind the following takeaways:

- Although the CMMC may not formally impact many contracts in the short-term, contractors would be wise to begin familiarizing themselves with the CMMC and working to implement its requirements, starting with developing a plan of action and milestones ("POAM") and system security plan ("SSP"). Companies that implement the CMMC will be well positioned to compete for future DoD contracts incorporating these obligations – with solicitations being released as early as the latter part of 2020 – and requiring authorizations to operate ("ATOs") while those that do not incorporate the CMMC will find themselves ineligible for award.
- Costs associated with becoming CMMC certified are "allowable, reimbursable cost[s]."[37] Contractors can expect to be able to allocate CMMC certification costs indirectly across their DoD contracts, but the extent of the costs covered remains to be seen. Costs associated with the actual certification process (i.e., costs incurred from the time a contractor requests that a CMMC-AB-accredited assessor certify that the contractor has implemented relevant CMMC practices and processes) will likely be allowable and thus reimbursable. However, it is not clear whether costs of becoming CMMC compliant (i.e., the costs associated with implementing relevant CMMC practices and processes) will be considered allowable.
- The CMMC will introduce new litigation risks. In the procurement process, contractors should expect cybersecurity to play a larger role in DoD procurements, including best-value determinations,[38] and can

---

[36] Jason Miller, *Why DoD's Decision to make cybersecurity an 'allowable cost' matters*, Federal News Network (June 17, 2019), https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/.

[37] CMMC FAQs, *supra* n.12, at Question 19.

[38] Catherine R. Tucciarello, *et al.*, *"Help Me, Help You": Defense Department Advises Contractors That Cybersecurity Is An Allowable Cost*, Nat'l L. Rev. (June 24, 2019), https://www.natlawreview.com/article/help-me-help-you-defense-department-advises-contractors-

expect bid protests implicating cybersecurity concerns to increase for DoD procurements. Defense contractors that fail to satisfy applicable CMMC requirements or to maintain their systems to remain in compliance could face contract claims under the Contract Disputes Act and False Claims Act liability.

- The CMMC will have extensive impacts on contractors' supply chains. Defense contractors will need to ensure that they incorporate the CMMC requirements into their subcontracts and verify that their subcontractors have in fact complied with the CMMC and received the requisite certifications.
- Although the CMMC establishes a consolidated framework of security controls, defense contractors will remain subject to existing compliance obligations. For example, the CMMC does not obviate the safeguarding or cyber incident reporting requirements established in DFARS 252.204-7012. Rather, the CMMC establishes a mechanism for demonstrating compliance with the safeguarding provisions of the rule, which remain in effect and builds upon those requirements.

---

cybersecurity-allowable-cost (" 'We cannot look at security and be willing to trade off to get lower cost, better performing product or to get something faster. If we do that, nothing works and it will cost me more in the long run.' " (quoting Katie Arrington, DoD's Chief Information Security Officer for the Assistant Secretary for Defense Acquisition)).