DRAFT
1.12.2021

Protectionism or Perfectionism: Exploring The International Trade Implications of DoD's Cybersecurity Maturity Model Certification

Jayme C. Selinger

Jayme Selinger is a Contract Law and Intellectual Property Specialist at MIT Lincoln Laboratory. He holds a law degree from the University of New Hampshire School of Law and is enrolled in an LL.M. program in government contracts from The George Washington University Law School.

The views, thoughts, and opinions expressed in this paper belong solely to the author and not to the author's employer or any other group or individual.

Abstract

DoD is addressing growing cybersecurity concerns with its contractor base by introducing a new cybersecurity certification requirement known as the Cybersecurity Maturity Model Certification (CMMC). CMMC supplements existing cybersecurity requirements known as the NIST SP 800-171 by imposing additional requirements on DoD contractors. CMMC was not developed transparently or with international input and is at odds with well-established international trade obligations. This paper will explore the international trade implications of CMMC and suggest that important reforms to CMMC need to be made before international partners force DoD's hand.

I. Introduction

When it comes to cybersecurity, China and Russia pose grave threats to the United States and its allies, but is the U.S. Department of Defense (DoD's) Cybersecurity Maturity Model Certification (CMMC) the answer to combatting this threat? The CMMC ruleset will force all U.S. defense contractors, domestic and foreign, to become certified to the Defense Department's cybersecurity standards, processes and practices with the exception of commercial off the shelf providers.[1] But cybersecurity is a dynamic and evolving practice with many different solutions.[2] Care must be taken to ensure both effective cybersecurity postures are adopted while also strengthening DoD's relationships with its defense contractor base. Unfortunately, DoD's current CMMC approach complicates these relationships and raises a serious barrier to entry into the Defense Department's massive public procurement market.[3]

The CMMC initiative was the result of two major challenges. The first challenge was that the current DoD cybersecurity rule, DFARS 252.227-7012, was based on a system of trust with little in the way of verification.[4] DoD found that this was problematic as it did not have true insight into how well its contractors were complying with the clause and essentially had a low confidence across its defense industrial base with respect to compliance.[5] The second challenge was that DoD

[1] *See generally* 85 Fed. Reg. 61505 (Sept. 29, 2020).
[2] *See* report from Aerospace Industries Association stating that "the Aerospace and defense industry supports DoD's efforts to protect against the proliferating cyber threat, but that DoD's implementation of NIST SP 800-171 constitutes a static solution to a dynamic problem." Aerospace Industries Association, Cybersecurity, https://www.aia-aerospace.org/issue/cyber-security/.
[3] *See* Chris Yukins, GW Law Webinar – A Tumultuous Year for Trade, Public Procurement International, September 3, 2020, https://publicprocurementinternational.com/category/defense/.
[4] Inspector Gen., Dep't of Def., Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, Rep. No. DODIG-2019-105 (July 23, 2019).
[5] *See* 85 Fed. Reg. 61505, *supra* note 1, at 61508, stating "DFARS clause 252.204–7012 does not provide for the DoD verification of a DIB contractor's implementation of the security requirements specified in NIST SP 800– 171 prior to contract award. DIB companies self-attest that they will implement the requirements in NIST SP 800–171 upon submission of their offer. Findings from DoD Inspector General report (DODIG–2019–105 ''Audit of Protection of DoD Controlled Unclassified Information on Contractor- Owned Networks and Systems'') indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI

found the cyber threat to be persistent and growing so rapidly that the Defense Department could no longer rely on the current cybersecurity standards to address these additional threats.[6] This resulted in an interim CMMC requirement that created far more questions than answers.[7] Some of the most difficult questions stemmed from how DoD intends to apply CMMC to vendors from the United States' international allies and partners.[8] This paper will discuss the background leading up to CMMC and then explore the international consequences of CMMC, including trade barriers and inconsistencies with United States obligations under its international trade agreements.

The discussion below will begin with the legislative history leading up to CMMC and DoD's justification for its interim release. It will then provide an overview of the CMMC structure and requirements, which were hand-picked by DoD in a non-transparent manner. It will then focus on CMMC and United States obligations under international trade agreements and conclude that CMMC serves nationalistic policies and is a form of protectionism. Finally, the discussion will examine a number of potential international responses to CMMC which may force DoD to reassess its approach. Several recommendations are also provided at the end which stress the need for international participation with CMMC including the need for equivalent standards.

---

and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds the element of verification of a DIB contractor's cybersecurity posture through the use of accredited C3PAOs. The company must achieve the CMMC level certification required as a condition of contract award."

[6] *See* 85 Fed. Reg. 61505, *supra* note 1, at 61508.

[7] CMMC was published as an Interim Rule under FAR 1.501-3(b) authority that states "[a]dvance comments need not be solicited when urgent and compelling circumstances make solicitation of comments impracticable prior to the effective date of the coverage, such as when a new statute must be implemented in a relatively short period of time. In such case, the coverage shall be issued on a temporary basis and shall provide for at least a 30 day public comment period." The American Bar Association Public Contract Law Section drafted a letter to DoD leaders offering comments in response to the Interim Rule which discuss various issues with its current wording. *See* Federal Acquisition Case 2019-D041-Comments on Interim Rule to Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, November 23, 2020, https://www.americanbar.org/content/dam/aba/administrative/public_contract_law/comments/dfars-cmmc-contractor-implementation-cyber-20-11-23.pdf [hereinafter ABA Public Law comments].

[8] *See* ABA Public Law comments, *supra* note 7.

A. Standardizing Cybersecurity Across DoD and the Defense Industrial Base

In 1996, the United States government passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which called for national standards to protect sensitive patient health information.[9] Building upon this success, the United States sought to protect information stored on government IT systems, and so Congress passed the Federal Information Security Management Act of 2002.[10] These IT standards applied to contractors that possessed or used federal information or that operated, used, or had access to federal information systems on behalf of an agency.[11] Agencies applied the information security standards to contractors by inserting language into each contract as deemed necessary but there was no specific Federal Acquisition Regulation (FAR) or Defense supplement (DFARS) clause available to reference.[12] A Government Accountability Office (GAO) study in 2005 found that agencies were not fully complying with FISMA requirements.[13] Nevertheless, FISMA was a key piece of legislation for cyber compliance in the federal government and it authorized the National Institute of Standards and Technology (NIST) to oversee cyber policy and create the original standards under NIST Special Publication (SP) 800-53 which was published in 2005.[14]

[9] *See* Centers for Disease Control and Prevention Publications & Resources, Health Insurance Portability and Accountability Act of 1996 (HIPAA), available at https://www.cdc.gov/phlp/publications/topic/hipaa.html.
[10] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, § 3541, 116 Stat. 2899, 2946 (2002) [hereinafter FISMA 2002)].
[11] *Id; See also* U.S. Gov't Accountability Off., GAO-05-362, Information Security over Contractors, (April 2005) [hereinafter GAO-05-362].
[12] GAO-05-362 at 3.
[13] *Id.*
[14] *See* FISMA 2002 Sec. 303; *See also* Nat'l Inst. of Standards & Tech., NIST SP 800-53, Recommended Security Controls for Federal Information Systems (2005) [hereinafter NIST SP 800-53].

NIST SP 800-53 centered around seventeen minimum security controls or "families"[15] and also distinguished between low-impact, moderate-impact, and high-impact information systems.[16] The highest-impact systems would store and process the most sensitive information.[17] The structure was set up such that each family contained additional controls and enhancements that were applicable based on whether the system would be designated as a low, medium and high-impact system.[18] This construct is still utilized today under NIST SP 800-53 rev. 5 which was most recently updated and republished in September 2020.[19]

By 2015, NIST had published SP 800-171,[20] which was intended to address how contractors should control information in nonfederal systems.[21] Additionally, the FAR now included a clause addressing basic safeguards for contractor information systems through.[22] DoD also issued DFARS 252.204-7012,[23] which was a contract clause that required contractors to comply with the controls identified in NIST SP 800-171. Both the NIST SP 800-171 and the DFARS 7012 clause were subsequently updated several times over the years with the latest

[15] The 17 families included: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. *Id.*
[16] *See* NIST SP 800-53 *supra* note 14.
[17] *Id.*
[18] Family number one was Access Control or "AC" and within this family were twenty controls known as AC-1 through AC-20. As an example of how the controls worked, AC-20 entitled "Use of External Information Systems," included one baseline control and one additional control for both medium and high-impact systems. The baseline control required the organization to establish terms and conditions for authorized individuals to: (1) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system. For medium and high-impact systems, AC-20 required prohibiting authorized individuals from using an external information system to process, store, or transmit controlled information. *Id.*
[19] Nat'l Inst. of Standards & Tech., NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations (September, 2020).
[20] Nat'l Inst. of Standards & Tech., NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (June 2015).
[21] FISMA was also repealed and replaced with the Federal Information Security Modernization Act of 2014, codified under 44 U.S.C. §§ 3551–3559.
[22] See FAR 52.204-21, Basic Safeguarding of Contractor Information Systems, (Jun 2016).
[23] Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69273 (Nov. 18, 2013).

versions being published on February 2020 for the NIST (rev. 2)[24] and December 2019 for the DFARS[25] clause.

In 2019, the Secretary of Defense asked its Inspector General (IG) to conduct a DoD-wide audit to determine whether contractors were protecting Controlled Unclassified Information (CUI) on their networks and systems in accordance with NIST SP 800-171.[26] The IG found that "DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information."[27] The IG report recommended that DoD validate annually a contractor's ability to protect CUI and DoD information.[28] The IG report also recommended that DoD Component contracting offices be required to validate contractor compliance with minimum security requirements.[29] This provided a solid basis for DoD to implement CMMC as soon as possible.

i. DoD's Cybersecurity Maturity Model Certification (CMMC)

Even before the IG report was released, DoD had been already been working on a companion piece to the NIST SP 800-171 known as the Cybersecurity Maturity Model Certification or "CMMC".[30] The IG report simply confirmed DoD's suspicions and gave it an

[24] *See* Nat'l Inst. of Standards & Tech., NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (February 2020).
[25] *See* DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (Dec 2019).
[26] Inspector Gen., Dep't of Def., Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, Rep. No. DODIG-2019-105, July 23, 2019, https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/) [hereinafter IG Report].
[27] IG Report at Findings.
[28] IG Report at Recommendations.
[29] *Id.*
[30] The IG Report was published in July 2019 but in early 2019 DoD asked the Software Engineering Institute (SEI) and to help make a maturity model for DIB cybersecurity. *See* Software Engineering Institute, Building the Cybersecurity Maturity Model Certification, July 28, 2020, https://www.sei.cmu.edu/news-events/news/article.cfm?assetid=644398.

excuse to roll out CMMC earlier than expected.[31] The CMMC model builds upon the NIST SP 800-171 by adding a scalable certification to verify the implementation of additional CMMC processes and practices as well as the NIST SP 800-171 controls associated with a corresponding maturity level. What this means is that contractors must have an appropriate certification level commensurate with the level of risk identified by DoD in the solicitation at the time of contract award. The table below shows what is required under CMMC for each level.[32]

CMMC Level	Description of Controls
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204-21.
2	Consists of 65 security requirements from NIST SP 800-171 implemented via DFARS clause 252.204-7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800-171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800-171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800-171, 61 CMMC practices, and 5 CMMC processes.

The CMMC maturity levels will range from one to five and will be identified in Sections L and M of DoD requests for proposal. For Level one, CMMC only requires certification to the basic safeguarding clause in the FAR.[33] This clause contains 15 basic controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

[31] *See* ABA Public law comments, *supra* note 7. Importantly, DoD planned to implement CMMC on a rolling basis by targeting "pathfinder programs" which will require various CMMC levels each year until 2025 when it expects *all* solicitations to require CMMC certification. Jared Serbu, Pentagon Ready to Name First 15 'Pathfinder' Contracts for CMMC, December 3, 2020, https://federalnewsnetwork.com/defense-main/2020/12/pentagon-ready-to-name-first-15-pathfinder-contracts-for-cmmc/.
[32] *See* 85 Fed. Reg. 61505, *supra* note 1.
[33] *See* FAR 52.204-21, *supra* note 22.

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

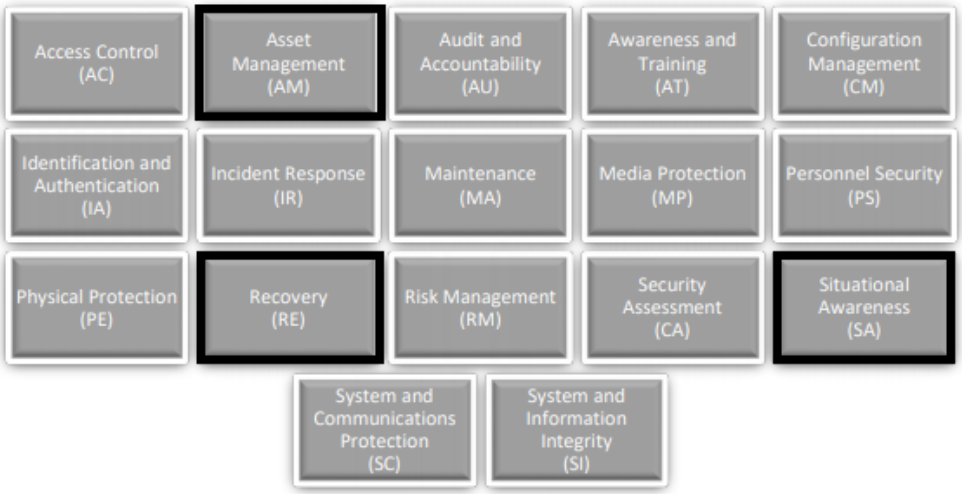
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Level one therefore is about protecting information systems as opposed to the information itself.[34] Additionally, level one is not tied directly to NIST SP 800-171 and it only requires what DoD considers to be the most basic form of practicing cybersecurity.[35] Nevertheless, DoD will require that all contractors become certified to these standards by an outside assessment organization.[36] In fact, CMMC imposes a certification requirement at *all* levels by an accredited member of the CMMC Third Party Assessment Organization (C3PAO).[37] C3PAOs are accredited by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB), which is an independent nonprofit organization contracted by DoD to oversee the C3PAOs and will be the sole body responsible for the CMMC assessor accreditation program for DoD.[38]

While level one only requires certification to the FAR requirements, Levels two through five will require certification to the NIST SP 800-171 standards as well as additional CMMC standards. CMMC has borrowed various standards from the FAR, DFARS, NIST, ISO, and

[34] *See* Reginald M. Jones, Mary Mikhaeel, Cybersecurity: How to Successfully Navigate CMMC and the DFARS, American Bar Association Public Contract Law Section, Procurement Lawyer Summer 2020, Vol. 55, No. 3 (discussing the history of the FAR requirements and noting the that the FAR Council published the FAR rule to implement a rule to protect information systems, as opposed to information itself.).
[35] *See* 85 Fed. Reg. 61505, *supra* note 1, at 61506.
[36] *Id.*
[37] *Id.*
[38] The Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB) signed a Memorandum of Understanding (MOU) with DoD in March 2020. The MOU sets forth the understandings held by DoD and the CMMC-AB regarding CMMC accreditation, certification, approval, training and assessment processes. *See* Memorandum of Understanding between The Department of Defense, Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB), March 17, 2020, available at https://www.ndia.org/-/media/sites/ndia/policy/blog/documents/cmmc-ab-mou.ashx?la=en&utm_campaign=Newsletter%20of%20Assurity%20Drive&utm_medium=email&utm_source=Revue%20newsletter.

Aerospace Industrial Association National Aerospace Standards – essentially creating a hodge-podge of hand-picked new standards.[39] Interestingly, the CMMC framework is rooted in seventeen domains of technical capabilities, fourteen of which are borrowed directly from NIST SP 800-171. The three domains highlighted below are new requirements contained in the CMMC model framework:[40]



The way that CMMC is setup is that each domain consists of a set of processes, capabilities and practices. The diagram below illustrates this structure.[41]

[39] *See* Jones, *supra* note 34, at 34.
[40] Cybersecurity Maturity Model Certification (CCMC) ver 1.02, March 18, 2020 at 7.
[41] *Id.* at 3.

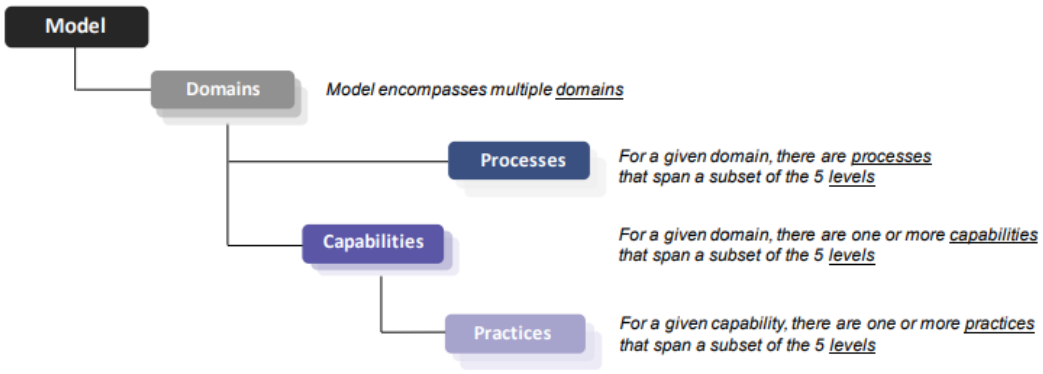


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

There are forty three capabilities associated with the seventeen domains.[42] Capabilities are achievements to ensure cybersecurity objectives are met within each domain.[43] Examples of capabilities include establishing system access requirements, conducting training and planning and conducting incident response testing.[44] Capabilities require practices, which are defined as specific *technical* activities that are required and performed to achieve a specific level of cybersecurity maturity for a given capability domain.[45] Practices range from "Basic Cyber Hygiene" to "Advanced/Progressive." Level one practices are called "Basic Cyber Hygiene" and are consistent with protecting Federal Contract Information (FCI) and correspond to the basic safeguarding requirements in the FAR.[46] Level three practices are called "Good Hygiene" and focus on the protection of CUI and as well as all NIST SP 800-171 controls.[47] Level five practices are called "Advanced/Progressive" and focus on the protection of CUI from "Advanced Persistent

[42] *Id.* at 7.
[43] *Id.* at 8.
[44] *Id.*
[45] Andrew Hoover, Cybersecurity Maturity Model Certification (CMMC) Part 2: Process Maturity's Roles in Cybersecurity, June 1, 2020, https://insights.sei.cmu.edu/sei_blog/2020/06/cybersecurity-maturity-model-certification-cmmc-part-2-process-maturitys-role-in-cybersecurity.html#:~:text=Within%20CMMC%2C%20practices%20and%20processes,given%20capability%20in%20a%20domain.
[46] *See* CMMC v.1.02, *supra* note 40, at 4.
[47] *Id.* at 6.

Threats."[48] And whereas a practice is a *technical* activity, a process is a specific *procedural* activity that is required and performed to achieve a maturity level.[49] There are five processes across the five CMMC levels ranging from "Performed" to "Optimizing."[50] A level one process is called "Performed" which means that an organization performs the specified practices but does not require documentation for these practices.[51] A level three process is called "Managed" and requires an organization to establish and maintain a plan for level three practices.[52] A level five process is called "Optimizing" which means the contractor is expected to "optimize" all processes across its organization including the previous processes.[53] The chart below helps to visualize this structure.[54]

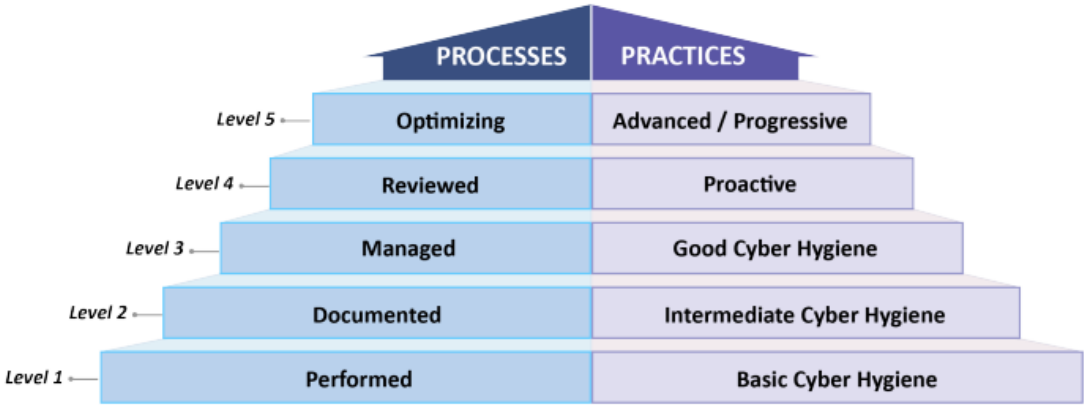


Figure 2. CMMC Levels and Descriptions

It is important to understand why DoD felt compelled to include these additional requirements in addition to the NIST controls. According to the Software Engineering Institute (SEI), one of the chief architects of the CMMC maturity model, the twenty added practices within CMMC levels one through three enhance the overall security posture of defense industrial base

[48] *Id.* at 7.
[49] *See* Hoover *supra* note 45.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *See* CMMC v. 102 *supra* note 40.

(DIB) organizations.[55] The practices are thought to add benefits above and beyond the NIST. Specifically, the practices (1) create a way to progress in cybersecurity capabilities; (2) they add mechanisms to address specific and common threats; (3) enable organizations to become more proactive in cybersecurity capabilities; and (4) introduce sustainment activities that can help organizations maintain operations in the event of disruption.[56] A few examples below illustrate how CMMC practices are designed to supplement and enhance the NIST controls based on three distinct categories:[57]

Category 1: Foundational practices to assist DIB companies in advancing their cybersecurity programs.

Example: *AU.2.044--Review audit logs*. Multiple practices in NIST SP 800-171 deal with capturing audit logs, but none specifically requires the review of audit logs, which is a foundational practice for auditing and accountability. An audit log is important because logs contain records related to computer security and can track user authentication attempts and security device logs that record possible attacks.[58]

Category 2: Practices that increase situational awareness to proactively identify and mitigate risks.

Example: *R.2.097--Perform root-cause analysis on incidents to determine underlying causes*. The purpose of this practice is to determine the underlying causes of events or problems to prevent the issue from reoccurring. Root-cause

[55] *See* Hoover *supra* note 45.
[56] *Id.*
[57] Andrew Hoover, Beyond NIS TSP 800-171: 20 Additional Practices in CMMC, June 22, 2020, https://insights.sei.cmu.edu/sei_blog/2020/06/beyond-nist-sp-800-171-20-additional-practices-in-cmmc.html.
[58] *See* Nat'l Inst. of Standards & Tech., NIST SP 800-92, Guide to Computer Security Log Management, (September 2006) at 2-1.

analysis is not explicitly mentioned in NIST SP 800-171 or in the "Computer Security Incident Handling Guide," which NIST SP 800-171 refers to. Root cause analysis is a best practice and is defined as a "principle-based, systems approach for the identification of underlying causes associated with a particular set of risks."[59]

Category 3: Practices that enhance protection and sustainment against common threats to the DIB, such as phishing, ransomware, and malware.

Example: *RE.2.137--Regularly perform and test data backups.* As mentioned, NIST SP 800-171 focuses on the confidentiality of CUI data. The ability to recover and restore data after an incident or disaster is also an important element of a robust cybersecurity program to combat ransomware attacks as well as unintentional incidents that may cause an organization to lose access to production systems and/or data.

CMMC will become a requirement for all DoD contracts by October 2025 and every DoD contractor must become familiar with the NIST SP 800-171 standards as well as the new CMMC processes and practices unless the contract is solely for commercial off the shelf items. CMMC is therefore adding another layer of complexity and cost on top of an already complex and expensive-to-implement NIST standard. It appears that CMMC is also attempting to boost the NIST standards which calls into question whether or not the current NIST standards alone are adequate and why NIST was not responsible for improving these standards.[60] CMMC is therefore ripe for

[59] *See* Nat'l Inst. of Standards & Tech., NIST SP 800-30, Guide to Conducting Risk Assessment, (September 2012) at B-10.

[60] *See generally* 85 Fed. Reg. 61505, *supra* note 1 noting although the security requirements in NIST SP 800-171 address a range of threats, additional requirements are still needed.

controversy, especially within the international community, where it can be seen as protectionism and contrary to current United States trade obligations.

II. International Trade Implications

The United States is estimated to have awarded more than $559 billion in public procurement contracts for FY 2018 with about $373 billion being attributed to DoD.[61] International trade agreements help facilitate access to procurement markets such as the United States', by establishing legally binding ground rules for equal treatment and participation by member countries.[62] The United States has played a key role in developing trade agreements that open up government procurement to international competition.[63] One of the main agreements is the World Trade Organization's Government Procurement Agreement (GPA) which facilitates billions in foreign contracts and is therefore a good place to start examining the legality and practicality of CMMC.[64]

A. The Government Procurement Agreement and CMMC

The GPA is a plurilateral agreement operating within the World Trade Organization's (WTO) framework.[65] Not all WTO members are parties, in fact, there are 20 parties comprising 48 WTO members and 36 WTO member/observers as well 12 members going through the process

[61] Andrew Eversden, New Data Shows the Soaring Cost of Government Contracts, August 1, 2019, https://www.federaltimes.com/newsletters/acquisition-update/2019/08/01/government-spent-nearly-560-billion-on-contracts-in-2018/.
[62] Yukins, Christopher R. and Schnitzer, Johannes, GPA Accession: Lessons Learned on the Strengths and Weaknesses of the WTO Government Procurement Agreement (2015). 7 Trade Law & Development Journal 89 (India 2015), GWU Law School Public Law Research Paper No. 2015-64, GWU Legal Studies Research Paper No. 2015-64, Available at SSRN: https://ssrn.com/abstract=2749889.
[63] U.S. Gov't Accountability Off., GAO-19-414, International Trade, Foreign Sourcing in Government Procurement, (May 2019) at 1 [hereinafter GAO-19-414].
[64] *Id.*
[65] *Id.* at 5.

of acceding.[66] GPA parties are estimated to have opened public procurement activities worth about $1.7 trillion annually.[67] Each party is required to abide by an overarching set of minimum standards for public procurement, including open, fair and transparent conditions of competition.[68] Nevertheless, these standards apply only to certain procurements through affirmative commitments made by the parties, and those commitments are further dependent on specified thresholds (including monetary thresholds).[69] These affirmative commitments are memorialized in the parties' coverage schedules which are contained in Appendix 1 to the GPA.[70] The schedule of each party contains several annexes outlining a party's commitment with respect to four areas of coverage: (1) the procuring entities covered by the GPA; (2) the goods, services, and construction services covered by the GPA; (3) the threshold values above which procurement activities are covered by the GPA; and (4) exceptions to the coverage.[71] Furthermore, a national security exception is provided for under Article III and is reproduced below.[72]

> Article III – Security and General Exceptions
>
> 1. Nothing in this Agreement shall be construed to prevent any Party from taking any action or not disclosing any information that it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or

[66] *See* Parties, Observers and Accessions, World Trade Organization, https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm, (last visited Dec. 9, 2020).
[67] Robert Anderson, Christopher Yukins, Withdrawing The U.S. From the WTO GPA: Assessing Potential Damage to the U.S. And Its Contracting Community, vol. 62 Gov't Contractor para 35, Feb. 12, 2020, at 1.
[68] *See* Overview of the Agreement on Government Procurement, World Trade Organization, https://www.wto.org/english/tratop_e/gproc_e/gpa_overview_e.htm (last visited Dec. 9, 2020).
[69] David Palmeter, Niall P. Meagher, WTO Issues Relating to U.S. Restrictions on Participation in Iraq Reconstruction Contracts, American Society of International Law, vol. 8, issue 29, Dec. 26, 2003, https://www.asil.org/insights/volume/8/issue/29/wto-issues-relating-us-restrictions-participation-iraq-reconstruction.
[70] *See* GPA Accession, *supra* note 62, at 94.
[71] *See* Coverage Schedules, World Trade Organization, https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm, (last visited Dec. 9, 2020).
[72] *See* Revised Agreement on Government Procurement, World Trade Organization, https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm, (last visited Dec. 9. 2020).

war materials, or to procurement indispensable for national security or for national defence purposes.

2. Subject to the requirement that such measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between Parties where the same conditions prevail or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent any Party from imposing or enforcing measures:
    a. necessary to protect public morals, order or safety;
    b. necessary to protect human, animal or plant life or health;
    c. necessary to protect intellectual property; or
    d. relating to goods or services of persons with disabilities, philanthropic institutions or prison labour.

Based on the wording of the national security exemption it appears as though CMMC could be narrowly justified by DoD and not be seen to violate the GPA as DoD has found that CMMC is necessary to protect valuable intellectual property.[73] Nevertheless, the exemption above does require that CMMC not be seen as a disguised restriction on international trade. Certainly, CMMC applies equally domestically and abroad, but it will most likely favor U.S. contractors who are more familiar with the U.S. NIST standards and who will also have more access to the United States government's resources – including direct access to the U.S. based third-party assessors.[74] In fact, small businesses are the lifeblood of the U.S. economy and DoD will make every effort to

[73] *See* 85 Fed. Reg. 61505, *supra* note 1, at 61505.
[74] *See* ABA Public Law comments *supra* note 7 (stating that the Interim Rule lacks adequate consideration of the challenges faced by foreign suppliers who will have little access to U.S.-based third-party assessors).

ensure its small business supply chain remains qualified to receive DoD awards.[75] Thus, CMMC has an element of protectionism built in by default. That is because it is a U.S. standard crafted for U.S. partners and offers no equivalency to any of the existing international standards – it is a pass or fail system at the moment.[76] And while the DFARS 7012 clause recognizes equivalencies, there are no equivalencies recognized by the CMMC model framework which is a fundamental problem with how it was setup.[77] It is also exorbitantly expensive to implement and requires ongoing costs to maintain both the certification level and the standards.[78]

Furthermore, the Trump administration has openly and vigorously touted its "America First" policies and CMMC is certainly consistent with this approach. In fact, the United States National Security Strategy in 2017 explicitly endorses America First as a foreign policy. [79] This type of foreign policy is a form of economic nationalism which prioritizes the interests of U.S. citizens over those in other countries. Understandably, U.S. economic dominance is a recognized national security goal, but cybersecurity requirements should not be the means to achieve such a

[75] *See* FAR part 19 Small Business Programs, which implements the Small Business Act. Under FAR Subpart 19.2, the policy states the following: "It is the policy of the Government to provide maximum practicable opportunities in its acquisitions to small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns. Such concerns must also have the maximum practicable opportunity to participate as subcontractors in the contracts awarded by any executive agency, consistent with efficient contract performance. The Small Business Administration (SBA) counsels and assists small business concerns and assists contracting personnel to ensure that a fair proportion of contracts for supplies and services is placed with small business." Conversely, the EU procurement system does not protect small businesses or have set asides and seeks to ensure fair and open competition for all business sizes across the EU. *See generally* Directive 2014/24/EU (February 26, 2014).

[76] The new CMMC contract clause is DFARS 252.204-7021 "Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement" and simply requires the contractor to have a CMMC certificate at the CMMC level required by the contract.

[77] *See* DFARS 252.204-7012(b)(2)(B) stating "The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

[78] *See* 85 Fed. Reg. 61505, *supra* note 1, at 61513. For level 5, DoD estimates that the cost for a small entity to support this is $110,090.80.

[79] *See* National Security Strategy of the United States of America, Dec, 2017, at 1, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

goal. And even if CMMC technically passes legal muster under the GPA, it is not as clear as to how CMMC will play out with regards to the many individual defense agreements established between the United States and its foreign partners which solely focus on defense market access.

B. Reciprocal Defense Procurement Agreements and CMMC

The United States enters into global defense cooperation partnerships and reciprocal defense procurement agreements (RDPs) with foreign countries on an individual basis. These agreements serve as a means of strengthening relationships with allies and obtaining foreign innovative technologies and are a key area of success for U.S. national security.[80] In fact, the United States has even codified some of these relationships under 10 U.S.C. § 2500 by creating the National Technology and Industrial Base (NTIB) designation which includes the United States, Canada, the United Kingdom, and Australia.[81] Presently, seven allied countries and NTIB members are actively participating in the F-35 Joint Strike Fighter Program.[82] Not surprisingly, the NTIB, along with other U.S. allies, consist of nearly 40% of the world's gross domestic product and are responsible for producing some of the world's most innovative technologies.[83] CMMC stands to reduce U.S. access to these innovative technologies, reduce interoperability with allied technologies, and ultimately weaken U.S. national security.

The United States currently has RDPs with twenty-six countries.[84] RDPs are memorialized through a Memoranda of Understandings (MOU) under which the DoD and the other country agree

[80] Cong. Research Serv., IF11311, Defense Primer: U.S. Defense Industrial Base 1 (Jan. 31, 2020).
[81] The term "national technology and industrial base" means the persons and organizations that are engaged in research, development, production, integration, services, or information technology activities conducted within the United States, the United Kingdom of Great Britain and Northern Ireland, Australia, and Canada. *Id.*
[82] *Id.*
[83] *Id.* These allied countries include Germany, South Korea, Singapore, Switzerland, and Sweden.
[84] *See* Reciprocal Defense Procurement and Acquisition Policy Memoranda of Understanding, Defense Pricing and Contracting, https://www.acq.osd.mil/dpap/cpic/ic/reciprocal_procurement_memoranda_of_understanding.html, (last visited Dec. 10, 2020).

on terms to increase collaboration between military departments and defense industries.[85] These MOUs often establish "mutual assurances for nondiscrimination in defense procurement."[86] Importantly, MOUs are not contracts and do not bind either country in the same way as a trade agreement.[87] Nevertheless, MOUs are binding understandings implemented in the DFARS[88] which may utilize the "public interest" exception under the Buy American Act to waive the domestic preferences.[89] And while the MOUs are intended to promote and establish equal treatment among the parties' covered goods and services there is no guarantee and there is no enforcement mechanism.[90]

RDPs are similar to the GPA. For example, they express the goals of nondiscrimination and transparency, contain rules governing public procurements and impose a national security exemption where appropriate.[91] In fact, the solicitation procedures in the DFARS forbid imposing unusual technical or security requirements solely for the purpose of precluding the acquisition of defense equipment from qualifying countries.[92] Nevertheless, RDPs offer much less focus on transparency and nondiscrimination and procurement rules are often less detailed. For example, many of the principles and rules governing procurements are just a few paragraphs. Article 2 of

[85] Drew B. Miller, Is it time to reform reciprocal defense procurement agreements?, Public Contract Law Journal, Fall 2009, Vol. 39, No. 1 (Fall 2009), pp. 93-111, 94.
[86] *Id.*
[87] U.S. Gov't Accountability Off., GAO-05-188, Federal Procurement: International Agreements Result in Waivers of Some U.S. Domestic Source Restrictions, (January 2005) [hereinafter GAO-05-188] at 9.
[88] *See* DFARS 225.03 for a list of "qualifying countries."
[89] *See* GAO-05-188, *supra* note 87.
[90] *See* U.S. Gov't Accountability Off., GAO/NSIAD-92-126, International Procurement, (March 1992) at 2. The results in brief of the report stated: "The MOUs do not ensure fair treatment for either U.S. or European contractors. Even though the United States waives the Buy American Act, it continues to place many restrictions on its offshore defense procurements. The allies said that although they seek to maximize competition, they reserve the right to direct contracts to domestic or other European sources."
[91] *See* Miller, *supra* note 85, at 102.
[92] See DFARS 252.872-3(d).

the Australian MOU with the United States Government is illustrative. This RDP specifically mentions that it is designed to: [93]

a. Remove barriers to procurements of supplies produced in the country of the other Government.
b. Accord industries of the other Government treatment no less favorable in relation to procurement than that accorded to industries of its own country.
c. Use contracting procedures that, as a minimum, allow responsible suppliers from each country to compete for procurement by the other Government.
d. Exchange relevant implementing regulations, policy, guidance, and administrative procedures.
e. Ensure that all controlled information, including proprietary technical data, and defense equipment released to industry pursuant to this Agreement, is used only for submitting offers for and performing defense contracts covered by this Agreement, except as authorized by the release Government and by the holders of rights to the information and equipment.

Article 5 of the Australian RDP addresses the procurement procedures. The procedures call for transparency and specificity as to what is being procured but the language used is very brief and aspirational. For example, regarding disputes, each government is required to review complaints and disputes and to expeditiously resolve them between it and suppliers. Thus, RDPs only offer the key principles for defense procurements but do not offer the specificity that larger trade agreements would normally address. Therefore, CMMC is not expressly prohibited under

[93] *See* Memorandum of Agreement Between the Government of Australia and the Government of the United States Concerning Reciprocal Defense Procurement, April 11, 2013, *available at* https://www.acq.osd.mil/dpap/Docs/mou-australia.pdf.

individual RDPs, but it is also most certainly not addressed in the procurement procedures and it appears to be a direct attack on the purpose of the RDPs, which is to establish free access to Defense Department procurements. It remains to be seen how each government will ultimately react towards CMMC.

C. International Responses to CMMC

To date there has been no strong condemnation of CMMC from the international community. This may be because it was just published September 29, 2020 and CMMC has yet to actually become a requirement for the majority of DoD procurements. It will also most likely go through several rounds of revisions, but the general requirement that contractors will have to comply with both the NIST and CMMC will likely not change. Katie Arrington, Chief of Information Security for Acquisition at DoD, is quoted as saying that "CMMC will become the basis for a global standard."[94] She went on to say "[o]ur anticipation is that if there is an overseas entity that needs to hold [controlled unclassified information], that we would definitely have a team that would be able to go over and evaluate their network."[95] Ellen Lord, Under Secretary of Defense for Acquisition and Sustainment also is quoted as saying "[t]he CMMC team is currently working with multiple countries including Canada, the U.K., Denmark, Italy, Australia, Singapore, Sweden and Poland as well as the EU cybersecurity body."[96] But no additional information has

[94] *See* Dwight Weingarten, CMMC Aims for 'Global Standard in Cybersecurity, Arrington Says, April 17, 2020, https://www.meritalk.com/articles/cmmc-aims-for-global-standard-in-cybersecurity-arrington-says/

[95] *See* Mariam Baksh, Officials are also still hammering out conflict-of-interest issues, as watchdogs flag failures in Defense acquisition practices, June 5, 2020, https://www.nextgov.com/cybersecurity/2020/06/dod-officials-cybersecurity-accreditation-partners-struggle-china-question/165969/.

[96] *See* Jon Harper, Just In: U.S. Allies Considering Adopting Pentagon's CMMC Cybersecurity Standards, March 4, 2020, https://www.nationaldefensemagazine.org/articles/2020/3/4/us-allies-considering-adopting-pentagons-new-cybersecurity-standards-for-industry.

been offered as to what this collaboration will look like or how CMMC will be implemented overseas. [97]

Another point of contention is that CMMC has been an entirely United States led effort with little transparency in how the standards were created and with no international representation.[98] In fact, there is international jurisprudence addressing the use of technical standards in public procurement. The Court of Justice for the European Union has stated that technical requirements cannot be discriminatory and must have been derived in a transparent way.[99] Additionally, the MOU between DoD and the Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB), requires leadership and internal staff to be U.S. Citizens.[100] Because of the transparency issues, the potential for discrimination, and the lack of international representation on the CMMC leadership board, the potential trade barriers could not have been fully understood and must be assessed as soon as possible.[101]

[97] *See* Baksh *supra* note 95. Stacy Bostjanick, director of cybersecurity policy for the Defense Intelligence Agency, said that the CMMC accreditation body is currently working through a process of establishing bilateral agreements to facilitate the program in allied countries. *Id.*

[98] There has been very little information available as to how the CMMC standards were developed.

[99] *See* Commission v. Netherlands, http://curia.europa.eu/juris/document/document.jsf?docid=122644&doclang=EN commonly referred to as the "Max Havelaar" case.

[100] *See supra* note 38.

[101] *Id.* The CMMC-AB touched on this point further in a request for information document looking for sources to support the creation and delivery of exams to evaluate and certify professionals in the CMMC ecosystem. In this document, it stated "CMMC-AB desires a global exam development and delivery solution and expects to partner with an organization who can deliver services around the globe and in multiple languages. CMMC-AB anticipates development of a majority of the content in the United States and in English. However, DoD and US Government operations across multiple countries, as well as future engagement with allied nations, result in an anticipated requirement to support professionals who seek to learn about CMMC in other countries and languages." CMMC-AB Certification Exam Development and Delivery Services Market Research, May 27, 2020, available at https://mcusercontent.com/6e7d7963b1219eb1b0fbda703/files/e29c047b-7714-4d27-bc85-b8eac1d17f59/CMMC_AB_Market_Research_Certification_Exam_Development_and_Delivery_Services_Final.pdf .

D. Forcing Change

There are a few avenues if international partners want to force change. First, because CMMC was issued on interim emergency basis, there was an opportunity up until November 2020 to provide comments back to DoD regarding the new rules.[102] DoD contractors can certainly voice their concerns and see if DoD is willing to address those publicly. For example, the DFARS 7012 clause has changed several times over the years and that is due to comments from industry.[103] Nevertheless, this is a very passive approach with little incentive for DoD to make actual changes unless there are numerous comments from the international community.

Secondly, international partners may adopt international standards for their procurements and require a similar certification process be conducted for access to their defense procurement markets. International standards set by the International Organization for Standardization (ISO) relating to cybersecurity such as ISO 27001 (Information Security Management) and ISO 27003 (Information Technology-Security techniques) are currently adopted by many organizations and may be a suitable alternative to the NIST and CMMC.[104] The European Parliament recently approved the proposal for a regulation on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") which introduces a cybersecurity certification framework for digital products, services and processes.[105] The Cybersecurity Act is based on the Directive on security of network and information systems "The NIS Directive" and was adopted

[102] The DFARS rulemaking procedures are governed by 41 U.S.C. § 1707, which generally requires DoD to issues a proposed rule for each rulemaking and to provide not less than a 30-day public comment period. In cases where this requirement is waived due to "urgent and compelling" circumstances, DoD may issue an interim rule but must provide at least a 30-day public comment period, and DoD may issue a subsequent final rule after considering any comments received. A final rule has not yet been issued.
[103] The DFARS clause has had several updates over the years from its original text in 2013.
[104] *See* ISO Standards are Internationally Agreed By Experts, available at https://www.iso.org/standards.html.
[105] *See* Regulation (EU) 2019/881 of April 17, 2019; *See also* The EU Cybersecurity Act, European Commission, February 28, 2020, available at https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

in 2016 and to become national law by 2018.[106] Title III of the Cybersecurity Act sets out a certification framework and establishes a harmonized approach to cybersecurity certification for certain products and services.[107] The certification is based on a comprehensive set of rules, technical requirements, standards and procedures."[108] Companies selling information and communication technology (ICT) products, services, and processes within the EU will already have to adopt these measures and achieve certification.[109] Therefore, DoD may have to reconcile these different requirements and it could quite possibly force acceptance of the EU approach as a CMMC equivalency.

Thirdly, countries may seek to bolster its own defense contractor base while shutting out the United States as a means of retaliation. For example, the European Commission has proposed expanding the European Defence Fund which seeks to bolster EU defense firms and cut out U.S. contractors from billions in European defense procurement contracts.[110] The new fund would be used to support defense innovation and development across Europe and bolster defense cooperation across EU firms.[111] This could be detrimental to many U.S. based contractors as it is estimated that eighty one percent of international contracts go to U.S. firms in Europe.[112]

---

[106] *See* Directive (EU) 2016/1148 of July 6, 2016; *See also* The Directive on security of network and information systems (NIS Directive), European Commission, October 9, 2020, available at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[107] *See supra* note 103.
[108] *See* Anastasios Arampatzis, What Is the EU Cybersecurity Act and What Does It Mean for US-Base Businesses?, August 30, 2020, https://www.tripwire.com/state-of-security/regulatory-compliance/eu-cybersecurity-act-united-states-based-businesses/.
[109] *Id.*
[110] *See generally* Christopher R. Yukins, European Commission Proposes Expanding The European Defence Fund – A Major Potential Barrier to Transatlantic Defence Procurement, 60 Gov't Contractor para 196, June 27, 2018.
[111] *Id.*
[112] *See* US Warns EU Over €13-billion Defense Spending, May 15, 2019, https://www.dw.com/en/us-warns-eu-over-13-billion-defense-spending/a-48738562.

Another countermeasure under consideration by the European Commission is the regulation of foreign subsidies.[113] Under its proposal, the EU would regulate its public procurement markets by banning foreign government subsidies and adding new grounds for exclusions that could target U.S. contractors.[114] The EU is concerned about market distortion and unfair competition through subsidies.[115] This could include U.S. contractors receiving COVID-19 relief under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act)[116] and therefore U.S. contractors could become excluded from EU procurements much like CMMC could exclude EU firms from U.S. procurements.[117]

III. Recommendations

For CMMC to be effective, DoD needs to renegotiate new bilateral agreements with its international partners to address cybersecurity requirements. These agreements must offer the flexibility to implement equally effective security controls and must be done in a way that is not so cost prohibitive that it creates a significant barrier to entry into the market. Defense contractors should be able to show equality of standards, using publicly available crosswalks between internationally recognized cybersecurity standards like ISO and those contained in the NIST. For example, NIST SP 800-53 rev. 4 contains a crosswalk chart between specific NIST controls and different equivalent standards.[118] CMMC is unique because it ignores existing crosswalks and simply picks and chooses requirements from the various standards. In fact, even NIST SP 800-171

---

[113] *See* Christopher Yukins, Comment on European Commission White Paper That Could Exclude "Subsidized" Foreign Vendors from EU Public Procurement, October 8, 2020, https://publicprocurementinternational.com/2020/10/08/european-white-paper/.
[114] *Id*.
[115] *Id*.
[116] *See* Pub.L. 116-136.
[117] *See supra* note 113.
[118] *See* NIST SP 800-53 rev 4. crosswalk which details the NIST control ID and maps the control to various other standards such as ISO27001/2:2013, available at https://it.nc.gov/documents/nist-800-53-security-controls-crosswalk.

allows contractors to implement alternative but equally effective security measures to compensate for the inability to satisfy a particular requirement whereas CMMC does not.[119]

There also needs to be international representation for CMMC both within DoD and the CMMC-AB body. The national security goals of the United States require international support and this cannot be done in a vacuum. Without some sort of equivalency process and international representation, the RDPs currently in place are meaningless and many otherwise qualified international partners will become automatically disqualified from DoD procurements.

IV. Conclusion

DoD stumbled when it published CMMC as an interim rule in September, 2020. It did not consider the full extent of CMMC and its impact on its longstanding obligations and relationships forged under international trade and reciprocal defense agreements. What DoD got right was that cybersecurity is a problem and it needs a dynamic solution. But CMMC in its current form, cannot be the solution because cybersecurity cannot just be checklist and it is not just a DoD problem. Industry has every incentive to protect its own valuable intellectual property and information from competitors and foreign adversaries just as much as DoD does. And therefore, equivalencies and international standards must be further examined and introduced into the CMMC process. Without this trust and flexibility, CMMC will just add to the towering bureaucracy in DoD without accomplishing its cybersecurity goals.

[119] *See* NIST SP 800-171 stating "To promote consistency, transparency, and comparability, compensatory security measures selected by organizations should be based on or derived from existing and recognized security standards and control sets, including, for example: ISO/IEC 27001/2 or NIST Special Publication 800-53."