COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

25 Sep 2019

Honorable Kevin Fahey
Office of the Assistant Secretary of Defense for Acquisition
3600 Defense Pentagon, Room 3E185
Washington, DC 20301-3600

Ref: Cybersecurity Maturity Model Certification V0.4

Dear Mr. Fahey:

The Council of Defense and Space Industry Associations (CODSIA)[1] is pleased to offer our comments in response to the Department of Defense (DoD) Request for Comment on the Cybersecurity Maturity Model Certification V0.4.

We have attached for your consideration our comments in the format you requested in the online announcement. Please note, this CODSIA submission reflects the inputs from many of the member associations and some associations will be directly providing more extensive submissions.

Thank you for your attention to these comments. If you have any questions or need any additional information, please contact Dave Drabkin, CODSIA at**:** codsia@codsia.org or by phone at: +1.703.927.1116.

Sincerely,

Steve Hall
Vice President, Government Affairs
American Council of Engineering Companies

Jimmy Christianson
Vice President, Government Relations
Associated General Contractors of America

[1] CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of seven associations – Aerospace Industries Association (AIA), American Council of Engineering Companies (ACEC), Associated General Contractors (AGC), Information Technology Industry Council (ITI), National Defense Industrial Association (NDIA), Professional Services Council (PSC), and U.S. Chamber of Commerce. CODSIA's member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

Ashley C. Berrang
EVP, Public Affairs
Information Technology Industry Council (ITI)

Wesley P. Hallman
Senior Vice President for Policy
National Defense Industrial Association

Alan Chvotkin
Executive Vice President and Counsel
Professional Services Council

Comment Template for Draft CMMC Model v0.4

Suspense for comments: 25 September 2019 at 1700 EDT

Send comments to the following email address: osd.pentagon.ousd-a-s.mbx.cmmc@mail.mil

	Point of Contact
First Name	Dave
Last Name	Drabkin
Organization	Council of Defense and Space Industry Associations (CODSIA)
Position	Administrator
Email address	codsia@codsia.org
Phone #	703.927.1116

*Comment Type: C: Critical; S: Substantive; A: Administrative

#	Comment Author	Comment Type (C,S,A)	Page	Domain	Capability	Practice or Process	Level	Comment (Including Rationale)	Suggested Change
1	CODSIA	S	NA	ALL	ALL	ALL	ALL	CMMC Rev. 0.4 was released on Sept 4. with comments due 21 days later on Sept. 25. As stated in the Overview Briefing, CMMC is intended to be a unified cybersecurity standard for all DoD acquisitions. A 21-day period during the last month of the fiscal year is an insufficient	CODISA respectfully requests a 60-day comment period for the next for public comment on CMMC Rev 0.6 that will be released in November. Extending the next comment period will allow us to have greater communication with a greater number of stakeholders, and

								timeframe to adequately review a rule that will impact all DoD acquisitions.	thus we will be able to provide more extensive comments on this proposed rule.
2	CODSIA	S	NA	ALL	ALL	ALL	ALL	There are more than half a million direct DoD Contractors or FTE. It is unclear how DoD expects this large number of contractors to be certified and in all DoD by next September. While this would be a challenge in of itself, critical guidance is missing, and the final version will not be released until January 2020 which will give DoD contractors mere months to come into compliance.	CODSIA respectfully requests more guidance and extended period before mandating CMMC in all DoD acquisitions. This will give companies time for certification and for DoD to issue clear guidance.
3	CODSIA	S	4	AC	C3	L5-3	L5	A service mediation layer is also commonly referred to as an Enterprise Service Bus. Is this how Government interprets a service mediation layer? How is a vendor expected to supply?	
4	CODSIA	C	4	AC	C5	L5-2	5	The concept of applying data obfuscation and deception is very broad.	Provide concrete examples as to how this might be implemented.

5	CODSIA	C	4	AC	C5	L5-3	5	Unsure what is meant by keeping CUI data cryptographically secure to include execution.	Data is typically encrypted in transit and when being stored. What is meant by encrypting data during execution?
6	CODSIA	C	7	AM	C1 Identify Assets	L1-1 • NIST SP 800-171 3.4.1 • RMM ADM:SG1.SP1	L1	This is a comprehensive requirement per the citations, which will be administratively intensive and will require regular updates to categorize "hardware, software, firmware, and documentation." Small businesses in particular may find the requirement prohibitive and/or onerous.	Don't include as part of Level 1
7	CODSIA	C	10	AA	C4 Auditing is performed	L1-1 • NIST SP 800-171 3.3.1	L1	This is a comprehensive requirement per the citations, which will be administratively intensive and will require extensive audit logs and records of regular "monitoring, analysis, investigation, and reporting" of	Don't include as part of Level 1

								activities. Small businesses in particular may find the requirement prohibitive and/or onerous.	
8	CODSIA	C	10	AA	C4 Auditing is performed	L1-1 • RMM MON:SG2.SP3	L1	Per the comment above, this is a comprehensive monitoring requirement that is administratively intensive. The citation elaborates detailed monitoring that would add to a small business' workforce requirements and likely be too onerous. The practice mentions "CUI" but at Level 1 it will likely be imposed on contractors that do not handle CUI.	Don't include as part of Level 1
9	CODSIA	C, S	11	AA	C7 Audit logs are reviewed	L1-1 • NIST SP 800-171 3.3.5	L1	The citation's use of the term "reporting" triggers questions related to identifying what to report, how to report, to whom to report, and where to	If the reporting requirement is meant to be only internal, then provide more detailed information about the process. If the reporting

								report. It also raises concerns about attribution. This is particularly important where DFARS 252.204-7012 is not applicable to a contract.	requirement is to external sources, then don't include as part of Level 1. The requirement raises significant issues and there must be better detail – in such cases, suggest only reporting well defined incidents and provide protection to the contractor concerning attribution and privacy.
10	CODSIA	C	16	CM	C3 Configuration baselines are established	L1-1 • RMM KIM:SG5.SP2	L1	This requirement is similar to NIST 800-171 3.4.1. The same comments above apply. The requirement will be too onerous for small businesses to comply.	Don't include as part of Level 1
11	CODSIA	S	19	CG	C2	Practice	L2-1	Define cybersecurity critical success factors.	

12	CODSIA	A	32	MP	C5	Practice	L3-1	Need clarity on control and maintenance on CUI outside controlled area. How can Security control in an open collaborative area? Example: WeWork space	
13	CODSIA	A	41	RM	C3	L5-1	L5	How will government/auditor assess “advanced automation and analytics capabilities”?	
14	CODSIA	C	43	RM	C6	Practice	L4-1	For small businesses that provide only Administrative Services at client site; will this apply?	
15	CODSIA	C	43	RM	C5	L5-3	5	Most organizations are not going to be able to hide the identity of a purchaser due to accounting and procurement requirements.	How are organizations supposed to accomplish this without the use of fronted delivery locations? Not sure what the advantage is of masking the purchaser other than preventing targeted tampering. There should be other mitigating factors in place, so it isn’t needed.
16	CODSIA	C	51	SCP	C1	L5-3	5	Employing zero trust concepts can be a never-ending spiral in	There needs to be an acceptable level of risk for all designs. There

								which nothing ever gets implemented.	will always be some level of risk present. Following a strict zero trust model ends up being expensive and counterproductive.
17	CODSIA	S	NA	ALL	ALL	ALL	ALL	If CMMC compliance is implemented post contract award, will vendor(s) be able to seek price adjustment or equitable adjustment?	
18	CODSIA	S	NA	ALL	ALL	ALL	ALL	Once CMMC is implemented, will Government select all controls within a specific level, or will there be a chance for some selection of different controls from different levels levied on any given contract?	
19	CODSIA	S	NA	ALL	ALL	ALL	ALL	How will Government go about selecting which level is appropriate for specified contract(s)?	
20	CODSIA	S	NA	ALL	ALL	ALL	ALL	Some controls seem to be specific to designing/maintaining a system as opposed to a business operation	

								system (i.e. O365). How will Government discern which controls are applicable to contract/company?	
28	CODSIA	S	NA	ALL	ALL	ALL	ALL	If the company leverages software as a service from other vendors, how are contract/government expected to investigate practice compliance and what if the third-party vendor is not able to reach required levels?	
29	CODSIA	S	NA	ALL	ALL	ALL	ALL	What will be the application process and requirements to become an auditor?	
30	CODSIA	S	NA	ALL	ALL	ALL	ALL	Will an auditor be able to provide compliance services and/or security management to a vendor doing business with the government whom is required to follow the CMMC requirements by the Government?	
31	CODSIA	S	NA	ALL	ALL	ALL	ALL	Will there be a centralized location or list of approved auditors that vendors are able to use?	

32	CODSIA	S	NA	ALL	ALL	ALL	ALL	Will auditors be on a contract with the government to provide respective services?	
33	CODSIA	C	N/A	N/A	N/A	N/A	N/A	Given the newness of the CMMC efforts, it is critical to provide "Best Practices" to industry based on initial assessments and experiences from early CMMC efforts as they continue to evolve.	Provide frequently updated "CMMC Best Practices" to industry based on early and ongoing pilot and evolving experiences.
34	CODSIA	C	N/A	N/A	N/A	N/A	N/A	FedRAMP certifications have proven to be neither inexpensive nor rapid to complete. Extensive efforts to streamline FedRAMP certifications have taken significantly longer than anticipated and still carry significant costs to participating companies. In addition, with CMMC controls likely to continue to evolve in relatively rapid fashion in response to dynamic threats, it is imperative to understand how DoD anticipates updating	Clearly call out how future content source changes (i.e., NIST-171, NIST-171 Rev B, DIB, ISO, CIS CSS, CERT RMM, etc.) will be incorporated into future versions of the certification process.

								capabilities and process requirements that must be met to receive future certifications.	