

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

CODSIA Case – 2024-001

February 26, 2024

Sent via the Federal eRulemaking Portal: <https://www.regulations.gov>

Ms. Diane Knight
Department of Defense
Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and
Transparency, Regulatory Directorate
4800 Mark Center Drive
Suite 08D09, Alexandria, VA 22350–1700
E-mail: osd.mc-alex.dodcio.mbx.cmmc-32cfr-rulemaking@mail.mil

**Public Comments by the Council of Defense and Space Industry Associations
(CODSIA) on DoD–2023–OS–0063, Cybersecurity Maturity Model Certification
(CMMC) Program Guidance**

Dear Ms. Knight:

On behalf of the members of the Council of Defense and Space Industry Associations (CODSIA), we write to submit these comments regarding the proposed rulemaking entitled “Cybersecurity Maturity Model Certification (CMMC) Program Guidance, Docket ID: DoD–2023–OS–0063, RIN 0790–AL49 published in the Federal Register on December 26, 2023.

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 eight associations – Aerospace Industries Association (AIA), Alliance for Digital Innovation, American Council of Engineering Companies (ACEC), Associated General Contractors (AGC), BSA, the Software Alliance (BSA), Information Technology Industry Council (ITI), National Defense Industrial Association (NDIA), and Professional Services Council (PSC). CODSIA’s member associations represent thousands of small and large 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.

CODSIA members are longstanding supporters of the Department of Defense’s (DoD’s) efforts to improve the security and resilience of the Defense Industrial Base (DIB). Our

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

CODSIA Case – 2024-001





member associations have engaged and counseled DoD leadership since the inception of the CMMC program and repeatedly provided actionable recommendations on ways to strengthen the program.

We were pleased to see that the proposed rule addresses many of the recommendations that were previously provided by industry stakeholders. We appreciate the rules' general alignment with the policy objectives that were communicated as part of the move from CMMC 1.0 to CMMC 2.0 and in subsequent engagements. We believe the rule provides much needed clarity on key questions, including the streamlining of Assessment Levels, a more flexible process of flowing down CMMC requirements to subcontractors, and a clearly defined roll out period that provides enough time for contractors to fully implement the program's requirements.

Next under, we have aggregated additional recommendations that impact our collective members, representing a significant portion of the Defense Industrial Base. Specifically, we recommend the following: 1) Ensure the protection of DoD data by delineating clear and actionable CUI marking instructions and responsibilities in contracts; 2) Future-proof the rule by defining a clear transition process for forthcoming standards revisions; 3) Specify assessment instructions and any applicable reciprocal procurement agreements for international subcontractors; and 4) Enable more flexible Plans of actions and milestones (POA&Ms).




If you have any questions or request additional information, please contact David Drabkin, the CODSIA Administrator, by email at codsia@codsia.org.

Sincerely,

 Lorenzo E. Williams Sr. Director, Acquisition Policy National Security Division Aerospace Industries Association	 Grant Schneider Senior Advisor Alliance for Digital Innovation
	
Steve Hall Vice President, Government Affairs	Jimmy Christianson Regulatory Counsel

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

CODSIA Case – 2024-001

American Council of Engineering Companies	Associated General Contractors of America
	
Gordon Bitko Senior Vice President of Policy, Public Sector Information Technology Industry Council (ITI)	Michael Seeds Senior Director Strategy and Policy National Defense Industrial Association
	
David J. Berteau President and CEO Professional Services Council	

CODSIA Case – 2024-001

Ensure the protection of DoD data by delineating clear and actionable CUI marking instructions and responsibilities in contracts.

Achieving CMMC’s desired risk management outcomes is contingent upon clear, accurate, and consistent CUI marking guidance. The current ambiguity in the marking process leads to significant marking inaccuracies. To minimize risk acceptance, many agency components default to overmarking data as CUI. This leads to a situation in which basic documents, presentations, and communications are incorrectly marked as CUI, which now must be protected per DFARS 252.204-7012. At the same time, the imprecise marking guidance provided to contractors potentially leaves true CUI unmarked, which goes against CMMC’s primary objective of protecting CUI in nonfederal systems. Per the National Archives’ website,¹ “agencies are responsible for marking or identifying any CUI shared with non-federal entities. [...] Contractors should not follow CUI program requirements or markings until directed to do so in a contract or agreement.” Accordingly, industry depends on the Department to identify, define, and describe the CUI requiring protection. This is especially true whenever the Department assigns the identification responsibilities to contractors. If the guidance is clear, accurate, and consistent, contractors can apply it to the data they generate for or at the direction of DoD and take necessary steps to ensure the protection of the data. This would also reduce the Department’s workload of responding to clarification requests from contractors. Without this critical information being defined to industry, there is a great risk of goal misalignment which could waste scarce resources at best and leave open vulnerabilities in sensitive systems at worst.

Future-proof the rule by defining a clear transition process for forthcoming standards revisions.

We appreciate the alignment of the CMMC controls to match those contained within the NIST Special Publication series on protecting CUI in non-federal systems. NIST is currently in the process of revising the SP 800-171 and SP 800-171A. As the requirements are being updated, this will change the assessment foundation for CMMC. The rule should clearly define how revisions to SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A will be handled.

To design a transition process that reflects advancements in security requirements while also being implementable, we offer the following input for your consideration. At the time of award, the contract should specify which revision applies. This should be the latest

¹

<https://www.archives.gov/cui/faqs.html#:~:text=Answer%3A%20Upon%20implementation%2C%20agencies%20are,to%20the%20government%20contracting%20activity.>

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

CODSIA Case – 2024-001

published version of the standard for which assessments are available. As NIST updates the underlying standards, there should be a clear roadmap for when the new requirements will go into effect. The transition timeline should account for the time it takes the Cyber AB to update the assessor training materials, train assessors, and have companies complete the updated assessment process. Before completing their new assessments, companies will also require time to reconfigure their systems to fully implement the new security requirements.

To bridge the gap between transitions, service level agreements (SLAs) or plans of actions and milestones (POA&Ms) may present suitable tools. Leveraging POA&Ms may necessitate additional revisions to the relevant section of the rule. Currently, POA&Ms are only allowed for initial assessments, not for situations in which the assessment baseline changes, which might cause some contractors to fall out of compliance.

Contractors who complete their tri-annual reassessments after the expiration of the appropriately scoped transition period should be required to certify to the latest version of the underlying standards.

Specify assessment instructions and any applicable reciprocal procurement agreements for international subcontractors.

CMMC requirements will need flowdown to all subcontracts. This includes international subcontractors, who will face additional challenges. Multinational DIB companies almost exclusively depend on local foreign national businesses to support contractual requirements in foreign countries. Thus, the rule as written is likely to have an impact on the ability of these multinational companies to fully support the DoD mission abroad. Please address how multinational corporations with facilities abroad supporting DoD clients and or non-US organizations (e.g., construction contractors abroad) are expected to comply with CMMC given US-centric aspects of some of the requirements (e.g., administrators, CAGE codes, etc...). Non-US companies may be unaccustomed to US-specific concepts like CUI and as such may not know how to train their personnel. We recommend providing specific guidance on how to cascade requirements to international subs with explicit mentions of any applicable reciprocal procurement agreements.

Enable more Flexible Plans of actions and milestones (POA&Ms).

We appreciate the decision to allow plans of actions and milestones (POA&Ms) for select controls during the CMMC assessment. We note that roughly two thirds of

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

CODSIA Case – 2024-001

objectives are not eligible for POA&Ms due to the excess risk that an incomplete implementation would introduce. We also note that after the closing of any applicable POA&Ms, the remaining 105 objectives will need to be maintained on a continuous basis to preserve the contractor's CMMC certification. As contractors need to update and reconfigure their systems, several controls pose an outsized challenge for small and medium sized contractors to maintain on a continued basis. We recommend providing greater flexibility on POA&Ms by allowing for extension requests for extenuating circumstances and by providing an option to maintain CMMC certification through an appropriate POA&M to close temporary deficiencies due to system reconfiguration.