4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

August 12, 2026

VIA ELECTRONIC SUBMISSION

TO: Department of Defense CMMC Reform Task Force

FROM: GovContractPros, LLC

RE: GCP Recommendations for Reforming CMMC and Reducing Compliance Burden for the DIB

GovContractPros, LLC ("GCP") appreciates the opportunity to provide comments in response to the Department of Defense (the "Department") Request for Information ("RFI") regarding the Cybersecurity Maturity Model Certification ("CMMC") program and potential reforms to reduce compliance burdens across the Defense Industrial Base ("DIB"). The Department's effort to solicit direct feedback from industry stakeholders demonstrates a commitment to strengthening cybersecurity while ensuring that acquisition policies remain practical, scalable, and supportive of innovation.

GCP advises dozens of organizations participating in the federal marketplace, including small businesses, mid-sized contractors, large prime contractors, and emerging non-traditional defense contractors. Through our work advising companies on federal compliance requirements, cybersecurity readiness, small business socio-economic certifications, contract management, and regulatory implementation, we have firsthand visibility into the challenges and opportunities associated with CMMC adoption across organizations of varying sizes, resources, and technical maturity levels.

Our clients collectively represent a broad cross-section of the DIB and span multiple sectors supporting the federal government. As a result, we are uniquely positioned to observe the practical impacts of CMMC requirements, including both the cybersecurity benefits achieved through implementation and the administrative, financial, and operational burdens experienced by contractors attempting to comply with evolving requirements.

We appreciate the Department's recognition that compliance costs and implementation challenges may disproportionately affect small, medium-sized, and non-traditional businesses, potentially limiting participation in the federal marketplace. We share the Department's objective of maintaining strong protections for Federal Contract Information ("FCI") and Controlled Unclassified Information ("CUI") while reducing unnecessary complexity, duplicative requirements, and barriers to entry.

The comments that follow are informed by our direct experience supporting defense contractors across the CMMC lifecycle and are intended to provide constructive, actionable recommendations that advance cybersecurity resilience, improve compliance efficiency, and strengthen the long-term health and competitiveness of the DIB.

Responses to Question 6:

The Department's RFI seeks specific and actionable policy changes or regulatory reforms to drastically reduce costs and barriers to entry without degrading the protection of federal data. Based on GCP's experience, the federal government currently faces a growing challenge in balancing the protection of CUI with the need to maintain a

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

competitive, innovative, and diverse industrial base. While the Department has developed the CMMC framework to validate contractor cybersecurity practices, other federal agencies have increasingly pursued separate cybersecurity initiatives, including the Department of Veterans Affairs ("VA") cybersecurity requirements, the Department of Homeland Security ("DHS") CUI safeguarding regulations, and the FAR Council's government-wide CUI rulemaking. These efforts share common objectives but risk creating multiple overlapping compliance regimes for contractors that support more than one federal agency.

The FAR Council's proposed CUI rule would establish government-wide protection requirements based on NIST standards, while DHS has implemented its own CUI safeguarding framework and Cybersecurity Readiness Factor, and VA has imposed separate cybersecurity, training, reporting, and compliance requirements through the VAAR. As a result, contractors increasingly face duplicative assessments, varying reporting requirements, multiple contract clauses, and inconsistent agency interpretations despite safeguarding the same underlying federal information.

This fragmentation disproportionately impacts small businesses, non-traditional contractors, venture-backed technology companies, and innovative commercial firms that lack the resources to sustain multiple federal compliance programs. The fragmentation harms the growth of external service providers that can meet one uniform standard. Rather than strengthening cybersecurity, duplicative compliance structures divert resources away from actual security improvements and toward administrative overhead.

Recommendation 1: Establish DoD as the Federal Lead Agency for Contractor Cybersecurity Certification

The CMMC Reform Task Force should recommend that the Department serve as the federal government's lead agency for contractor cybersecurity certification and assessment.

As the federal government's largest purchasing agency, the Department has administered NIST SP 800-171 requirements for nearly a decade and has already invested substantial public and private resources in developing assessment procedures, accreditation mechanisms, and certification processes through CMMC.

By creating uniform cybersecurity standards, the federal government benefits from a developing external service provider marketplace that can meet those cybersecurity needs for the small and medium sized business communities.

Rather than allowing each agency to create independent cybersecurity certification frameworks, the federal government should adopt a single certification recognized across all agencies. Contractors that successfully obtain a DoD cybersecurity certification should not be required to undergo separate cybersecurity assessments by DHS, VA, or other civilian agencies absent truly unique mission-specific requirements.

Recommendation 2: Create Government-Wide Reciprocity

The Task Force should recommend mandatory reciprocity throughout the federal acquisition system.

A valid CMMC certification should satisfy federal cybersecurity qualification requirements for all executive agencies handling CUI. This approach would mirror the successful model already utilized for socio-economic certifications in federal contracting. Federal agencies routinely rely upon SBA determinations regarding 8(a), HUBZone, and

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

SDVOSB eligibility rather than conducting separate certification reviews for every procurement. A similar "certify once, use everywhere" approach should apply to cybersecurity compliance.

Government-wide reciprocity would immediately reduce costs, decrease barriers to entry, eliminate redundant assessments, and promote consistency in contractor cybersecurity oversight.

Recommendation 3: Eliminate Agency-Specific Cybersecurity Evaluation Frameworks

The Task Force should recommend that agencies discontinue development of independent cybersecurity scoring, readiness, maturity, or assessment programs that duplicate CMMC or NIST-based evaluations.

For example, DHS's Cybersecurity Readiness Factor reflects many of the same objectives already addressed through CMMC and NIST 800-171 assessments. Maintaining multiple federal assessment methodologies increases compliance costs while providing limited additional security value.

A single federal assessment standard would provide greater consistency while reducing contractor uncertainty and administrative burden.

Recommendation 4: Limit Certification Requirements to CUI Exposure

The Task Force should recommend that cybersecurity certification requirements be imposed only where contractors actually create, receive, process, store, or transmit CUI.

Many small businesses performing low-risk support functions currently face uncertainty regarding future cybersecurity obligations despite never handling CUI. Compliance obligations should be narrowly tailored to encompass the actual risk of exposure and data access, thereby reducing unnecessary barriers to participation in federal contracting.

The Task Force should provide contractors with CUI marking guidance and clearly marking CUI when providing contractors with information. The DIB has many stories of the Department providing unnecessarily marked CUI or receiving information not clearly marked as CUI from the Department itself, from a prime contractor, or from subcontractors. Both represent a piece of regulatory red tape that the Department is capable of correcting through best internal practices. If the Department proactively provides the marking guidance so the DIB can understand which materials warrant increased protections, then the cybersecurity vulnerabilities in the DIB would be reduced.

Further, the Department should create guidance for prime contractors to provide subcontractors with only the necessary CUI for the completion of the contract activities. Costs on small subcontractors can be substantially reduced if the subcontractor only receives the information necessary to complete the contract. The Department can help by creating guidance that prime contractors can utilize to help reduce the burden of oversharing CUI to subcontractors and ensure such protection through licensed enclaves.

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

Recommendation 5: Expand Recognition of Existing Assessments

The Task Force should recommend broader federal acceptance of existing assessments as part of the business's Plan of Action & Milestones (POA&M), including:

- Prior DoD assessments;
- Federal Risk and Authorization Management Program ("FedRAMP") authorizations where applicable;
- Existing NIST-based independent assessments;
- Other federal cybersecurity attestations demonstrating equivalent protections.

Reducing redundant audits and leveraging existing assessment results to demonstrate the business's cybersecurity practices would significantly decrease costs for small and medium-sized businesses while maintaining the underlying security objectives.

Recommendation 6: Focus Oversight on Outcomes Rather Than Documentation

The federal government should prioritize protection of federal information rather than evaluating multiple overlapping plans, certifications, questionnaires, and reporting artifacts.

Contractors should be judged primarily on demonstrating implementation of required security controls, protecting CUI from compromise, and responding effectively to incidents. The Task Force can streamline, simplify, or reduce the numerous documentation components to CMMC. This approach would reduce compliance costs while preserving or improving security outcomes.

Recommendation 7: Certification of Joint Ventures

The Task Force should provide clear and uniform guidance regarding the application of CMMC assessment requirements to Small Business Administration ("SBA")-approved joint ventures.

For years, contractors have encountered inconsistent treatment regarding Facility Clearance Level ("FCL") requirements for joint ventures, especially from the Department itself. Despite SBA regulations recognizing many joint ventures as unpopulated entities that exist primarily for contract performance and management purposes, DoD components have at times continued to impose FCL requirements directly on the joint venture rather than evaluating the security capabilities of the individual joint venturers that actually perform the work. This issue has generated significant confusion, litigation, and inconsistent implementation across the DIB.

CMMC implementation presents a nearly identical challenge. The fundamental question is whether cybersecurity compliance should be assessed at the joint venture entity level or at the level of the joint venturers that own, operate, staff, and secure the systems used in contract performance.

In the case of an unpopulated joint venture, the joint venture itself frequently has no employees, no independent information technology environment, and no operational systems used to process, store, or transmit CUI. Instead, the underlying joint venturers provide the personnel, facilities, information systems, and cybersecurity infrastructure necessary for contract execution.

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

Accordingly, we recommend that the Task Force adopt a framework that evaluates compliance at the joint venturer level rather than requiring a separate assessment of the unpopulated joint venture itself. Where appropriate, the Government could recognize a licensed secure enclave or similarly controlled environment utilized by the joint venturers for contract performance and permit the assessment of the entities that actually own and operate the systems handling Federal information and CUI.

Such an approach would:

- Align CMMC implementation with the operational reality of unpopulated SBA joint ventures;
- Reduce unnecessary duplication of cybersecurity assessments;
- Avoid requiring the creation of artificial information technology environments solely to satisfy compliance requirements;
- Reduce barriers to participation by small business joint ventures, Mentor-Protégé joint ventures, and other collaborative business arrangements;
- Promote consistency with existing security and industrial-security practices; and
- Ensure that cybersecurity assessments focus on the entities actually responsible for safeguarding Federal information.

Most importantly, clear guidance is needed. Absent a uniform policy, contracting officers, assessors, program offices, and defense agencies may apply inconsistent standards across procurements, resulting in uncertainty, increased compliance costs, bid protests, and reduced participation by otherwise qualified contractors. The Task Force should therefore provide explicit direction regarding assessment obligations for joint ventures and clarify whether compliance responsibilities reside with the unpopulated joint venture entity, the individual joint venturers, or a combination of both.

We continue to recommend that the Department recognize secure-enclave solutions and permit CMMC assessments to be performed at the joint-venturer level where those entities provide the personnel, systems, facilities, and cybersecurity controls used in contract performance. This approach would strengthen security outcomes while reducing unnecessary administrative burdens and preserving competition within the DIB.

Recommendation 8: Commerciality of NIST/CMMC – Conversion to Non-COTS and the FAR

We respectfully encourage the Task Force, in coordination with the FAR Council, to evaluate the impact that CMMC certification requirements, CUI safeguarding obligations, cyber incident reporting mandates, and other Government-directed cybersecurity requirements may have on the commerciality determinations that form the basis of Federal procurement policy.

FAR 2.101 defines “commercial products” and “commercial services” based upon offerings that are customarily used by the general public or non-governmental entities and are sold, leased, licensed, or offered in the commercial marketplace. The Federal acquisition system has long recognized that commercial products and services should be acquired using procedures that reflect commercial market practices whenever possible.

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

Consistent with that policy, FAR 12.101 requires agencies to conduct market research to determine whether commercial products or commercial services are available to meet agency needs and directs agencies to acquire commercial products and commercial services when they are available.

As implementation of CMMC continues, an important policy question remains unresolved: at what point do Government-directed cybersecurity requirements fundamentally alter an otherwise commercial offering? Requirements relating to CMMC certification, CUI handling, Government-specific system security controls, cybersecurity reporting obligations, assessments, and other compliance mandates may impose obligations that are not customary in the commercial marketplace. In some circumstances, these requirements may effectively transform otherwise commercial products, commercial services, commercial supplies, or even COTS offerings into Government-unique solutions.

This issue is particularly significant because Federal law and acquisition policy establish a strong preference for commercial acquisitions. President Trump's Executive Order 14271, *Ensuring Commercial, Cost-Effective Solutions in Federal Contracts*, reaffirmed the Government's obligation to utilize commercially available products and services to the maximum extent practicable and to leverage the competitive commercial marketplace wherever possible.

Accordingly, we respectfully recommend that the Task Force, working in coordination with the FAR Council, undertake a formal evaluation of the extent to which CMMC requirements and other Government-unique cybersecurity obligations affect commerciality determinations under FAR 2.101 and FAR Part 12. The results of that evaluation should be translated into clear guidance for contracting officers so that acquisitions are structured consistently across the Department of Defense and the Federal Government.

Such guidance would benefit both industry and the acquisition workforce by:

- Clarifying when cybersecurity requirements remain consistent with commercial acquisition practices;
- Identifying circumstances where Government-directed requirements may render an acquisition non-commercial in nature;
- Promoting consistent commercial item determinations across agencies;
- Preserving access to innovative commercial suppliers and non-traditional contractors; and
- Ensuring continued compliance with Congress's and the Administration's preference for commercial products and commercial services whenever available.

Absent such guidance, contracting officers and the DIB may reach inconsistent conclusions regarding the impact of CMMC requirements on commercial acquisitions, resulting in uncertainty, reduced competition, and potential barriers to the participation of commercial firms in the federal marketplace.

Recommendation 9: The DoD should focus on clear implementation timelines

The Task Force should quickly announce a full pause of CMMC until the Task Force's recommendations are implemented. The pause in effect now does not meaningfully extend to the implementation date of CMMC Level 2. For small businesses, it is vital that the Department clearly and authoritatively states the intention to fully implement or pause the program. The Department's start and stop with the program has forced more investment in cybersecurity measures that are later met with external service providers. The Department has stated in the 2026 Unified Regulatory

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

Agenda the intention to update CMMC requirements to NIST SP 800-171 Rev 3. This further complicates the expected expenditures small contractors should be pursuing currently. The Task Force should create clear milestones and ensure compliance requirements are clearly explained to the small business community.

Recommendation 10: The DoD should meaningfully provide training and support to small businesses.

The Department has pledged during the implementation of CMMC to train and educate the small business community to ensure they continue participating in the DIB. The Task Force should recommend the Department provide meaningful in-person and virtual training opportunities to small businesses through a consolidated webpage specifically geared towards small businesses seeking to join or remain in the DIB.

Recommendation 11: Clear guidance for reimbursements of cybersecurity related costs

The Task Force should carefully evaluate the disproportionate economic impact that cybersecurity compliance requirements impose on small businesses as compared to "other than small" defense contractors.

While cybersecurity is an essential component of national security and protection of CUI, the cost burden associated with implementing, maintaining, documenting, and assessing CMMC compliance is not distributed evenly across the DIB.

Large defense contractors frequently perform work under cost-reimbursement, cost-plus, or other contract vehicles that permit the recovery of allowable compliance-related expenses through indirect cost structures and contract pricing mechanisms in accordance with FAR Part 31. In many cases, these contractors perform within sole-source or limited-competition programs where cybersecurity compliance costs can be incorporated into overhead pools, general and administrative expenses, and government-reimbursable contract costs.

By contrast, small businesses often compete in highly competitive environments where award decisions are driven by price and best value considerations under Firm-Fixed-Price ("FFP") contracts. Unlike large incumbents, many small businesses are required to absorb significant upfront investments in cybersecurity infrastructure, compliance personnel, assessment preparation, documentation, managed services, secure enclaves, and third-party assessment costs before any contract award is received.

As a result, CMMC compliance may function as a significant barrier to entry for small businesses because the costs associated with certification and ongoing compliance must frequently be priced into competitive Firm-Fixed-Price proposals. In a competitive procurement environment, those costs can place small businesses at a pricing disadvantage relative to larger firms that benefit from broader economies of scale or the ability to spread compliance costs across substantial portfolios of Government contracts.

This issue is particularly important in light of the Small Business Act's longstanding policy that small business concerns should receive a fair proportion of Federal contract opportunities and the FAR's requirement that agencies consider whether capable small businesses can satisfy Government requirements. The Government should be careful not to create compliance regimes that unintentionally restrict competition or diminish small business participation in the federal marketplace.

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

Accordingly, we recommend that the Task Force, in coordination with DoD, SBA, and the FAR Council, evaluate mechanisms to mitigate the disproportionate impact of cybersecurity compliance costs on small businesses. Such mechanisms could include:

- Recognition of shared or licensed secure-enclave solutions;
- Expanded reciprocity and reuse of existing assessments;
- Joint-venture and Mentor-Protégé assessment flexibility and permitting cost-reimbursement for CMMC and other CUI related costs under the Department's Mentor-Protégé Program;
- Greater use of phased implementation approaches;
- Clarification regarding allowable cost recovery mechanisms; and
- Acquisition strategies that account for the economic realities faced by small business contractors competing under Firm-Fixed-Price contracts.

The objective of CMMC should be to improve cybersecurity outcomes across the DIB, not to inadvertently favor large incumbent contractors whose compliance costs can be more readily absorbed or reimbursed through existing contract structures. The Department should therefore ensure that cybersecurity requirements strengthen security while preserving competition, innovation, and meaningful participation by small businesses.

Recommendation 12: The DoD can Rescind CMMC Requirements for small businesses through the Regulatory Flexibility Act

If the Department believes it has misunderstood the impact of the regulations on the small business community, then the Department is under the duty to completely rescind CMMC for the small business community since it inadequately estimated the impact. The Department can utilize 5 U.S.C. 610 or state the Regulatory Flexibility Analysis was insufficient so that small contractors may be relieved from the requirements while still maintaining large contractors' compliance. A delayed effective date for small contractors would permit the external service provider community to build market-ready solutions for CMMC compliance at low costs.

Recommendation 13: The DoD should certify businesses' compliance internally

The Department can make meaningful changes to the cost of CMMC compliance by providing certification through Department personnel rather than relying on the Certified Third-Party Assessment Organizations (C3PAO). The primary costs directly associated with CMMC are the costs associated with the C3PAO review. There are just over one hundred C3PAOs and scheduling an assessment can take months. Contractors often find difficulty in ensuring all documents are clearly captured before their assessment meeting with the C3PAO, requiring several more months of waiting for a follow-up assessment. If the Department wants to relieve businesses of financial hardship, providing certification as a government service would critically solve many issues with CMMC.

Based on our discussions with numerous small businesses, large businesses, and members of the broader DIB, the current CMMC assessment marketplace remains highly inconsistent with respect to both cost and scheduling. Many contractors report significant variability among C3PAOs, including widely divergent pricing structures, inconsistent

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

interpretations of assessment requirements, lengthy scheduling delays, and uncertainty regarding assessment readiness expectations.

As a practical matter, many contractors describe the current C3PAO environment as the "wild west." While the Department has invested significant effort in developing the CMMC framework, the assessment ecosystem remains largely dependent upon private-sector providers whose availability, pricing, and interpretive approaches may differ substantially from one assessor to another.

The Department has a unique opportunity to improve consistency, reduce costs, increase industry confidence, and strengthen cybersecurity outcomes by establishing a government-led assessment organization capable of performing CMMC assessments on behalf of the Department.

Such an organization could perform a role similar to that of the Defense Contract Audit Agency ("DCAA"). For decades, DCAA has served as the Department's independent audit organization, evaluating contractor business systems, accounting practices, indirect rates, and cost representations. Industry may not always agree with DCAA's findings, but contractors benefit from a centralized audit authority that applies a relatively uniform set of standards and interpretations across the DIB.

A comparable cybersecurity assessment organization could provide similar benefits by:

- Performing CMMC assessments on behalf of the Department;
- Establishing consistent interpretations of assessment objectives and security requirements;
- Reducing disparities in assessment outcomes among private assessors;
- Publishing lessons learned, best practices, and implementation guidance;
- Providing advisory support to contracting activities and program offices;
- Increasing transparency regarding assessment expectations;
- Reducing compliance costs, particularly for small businesses; and
- Creating a more predictable pathway to certification.

Such an organization would not necessarily need to replace private-sector C3PAOs. Rather, it could operate alongside the existing assessment ecosystem by serving as a government option for contractors, performing quality assurance reviews, providing appellate oversight, or conducting assessments in areas where private-sector capacity is limited.

This approach could be particularly valuable for small businesses. Unlike large defense contractors that are often able to spread compliance costs across extensive contract portfolios or recover certain costs through indirect rate structures, small businesses frequently compete under Firm-Fixed-Price acquisition models and must absorb significant compliance costs before contract award. A government assessment capability could help reduce barriers to entry while maintaining the integrity of the CMMC program.

Additionally, a centralized government assessment body would provide the Department with direct visibility into systemic compliance challenges across the DIB. Rather than relying exclusively on reports generated through multiple independent commercial assessors, DoD could identify recurring issues, develop standardized remediation guidance, and continuously improve the cybersecurity posture of its contractor base.

We therefore recommend that the Task Force explore the feasibility of establishing a DoD-led cybersecurity assessment organization, modeled in part after DCAA, that can perform CMMC assessments, promote consistency in

4445 Willard Ave, Suite 600
Chevy Chase, MD 20815
(o) 240.760.2902
www.govcontractpros.com

interpretation, provide best-practice guidance, and serve as a trusted resource for both industry and the acquisition workforce. Such an institution would improve uniformity, reduce costs, strengthen cybersecurity outcomes, and enhance participation by small businesses throughout the DIB.

In the alternative, the Department should establish Government-licensed, centrally managed CUI enclaves that contractors may lease on a subscription basis. These environments should include all technical, operational, and administrative safeguards necessary to satisfy CMMC Level 2 requirements. Contractors would be responsible only for user management, training, and operational use of the environment, while the Department would maintain control implementation, continuous monitoring, vulnerability management, infrastructure security, audit logging, and compliance reporting. This model would reduce compliance costs, improve cybersecurity consistency across the DIB, accelerate contractor participation, and enhance protection of CUI.

Conclusion

GCP appreciates the opportunity to provide these comments and recommendations regarding the future of the CMMC program. Our recommendations are guided by three overarching objectives: (1) strengthening the protection of FCI and CUI, (2) reducing unnecessary compliance costs and administrative burdens, and (3) preserving competition and participation throughout the DIB, particularly among small businesses, non-traditional contractors, and innovative commercial firms.

We believe these objectives can be achieved through greater standardization, government-wide reciprocity, clearer implementation guidance, expanded use of shared secure-enclave solutions, improved treatment of joint ventures and small businesses, and a renewed focus on cybersecurity outcomes rather than duplicative compliance processes. By simplifying requirements while maintaining strong security standards, the Department can improve both cybersecurity resilience and contractor participation across the federal marketplace.

We would like to sincerely thank the CMMC Reform Task Force, the Department of Defense, and all participating stakeholders for their willingness to engage directly with industry and solicit meaningful feedback on the future of the program. The collaborative approach reflected in this RFI demonstrates the Department's commitment to developing practical, effective, and sustainable cybersecurity policies. We appreciate the opportunity to contribute to this important effort and look forward to continued engagement as the Task Force evaluates potential reforms to strengthen both cybersecurity and the long-term health of the DIB.