



2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

August 14, 2026

Ms. Leanne Condren
Acquisition Directorate
RPN STE 12063 1155 Defense Pentagon
Washington, D.C. 203011000

Electronic Submission: leanne.m.condren.civ@mail.mil

Subject: Reforming CMMC and Reducing Compliance Burden for the DIB

Dear Ms. Condren,

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the Request for Information (RFI) on reforming the Cybersecurity Maturity Model Certification (CMMC) program and reducing compliance burden for the defense industrial base (DIB).

NDIA is the nation's largest defense industry association, representing over 1,600 corporate and over 66,000 individual members from small, medium, and large contractors, a majority of which are small businesses. NDIA members design, manufacture, apply, and maintain the cutting-edge technologies, systems, and platforms that our armed forces rely upon to deter aggression and defend our nation and its interests. As such, our members' professional and informed views on this request for information reflect the complexity and nuance of the issues under discussion.

NDIA and its member companies are committed to securing the data and systems that power the DIB, as well as the platforms, infrastructure, and services that support our nation's warfighters. Simultaneously, NDIA supports the efforts of the Department to review the impacts of the CMMC program to avoid extraneous costs and burdens on industry and focus resources and efforts to prioritize protecting the critical information and systems that truly matter.

In addition to the separate *2026 CMMC Survey* NDIA is conducting in coordination with the Department, data is included in this RFI response from a *DIB IT and Cybersecurity Survey* (Cyber Survey) NDIA conducted in April of 2024, which includes responses from 474 member companies of all sizes. Nearly three-quarters of the Cyber Survey respondents have contracted with the Department for over 10 years. 58% of the respondents were small businesses with less than 500 employees, and over one quarter (26%) had less than 49 employees. Finally, Attachment 1 includes a consolidated RFI response from NDIA's San Diego Chapter that consists of 48 respondents.

NDIA and its membership support the government's desire to promote a strong, dynamic, and robust defense industrial base. We thank you for the opportunity, and if you have any questions related to these comments, please reach out to Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association

Attachment: Consolidated Response from NDIA's San Diego Chapter

NDIA Response to Reforming CMMC and Reducing Compliance Burden for the DIB

1. Identify the top five most prohibitive cost drivers, administrative burdens, or operational challenges your organization has experienced, or anticipates to experience, when attempting to comply with the CMMC framework and NIST SP 800-171 Rev 2.

- **CUI Marking:** Industry continues to highlight multiple instances where inconsistencies, ambiguities, and inaccuracies within the current Controlled Unclassified Information (CUI) marking process lead to confusion, increased costs, and decreased security for all parties. The risk management goals of CMMC are fully dependent upon the ability of government and industry to effectively manage and safeguard defense-sensitive CUI. Effective management, however, is only possible with clear, accurate identification of what information requires protection, consistent government marking of CUI prior to the transmission of such CUI, and clear instruction to the contractor when their performance under a contract will create defense-sensitive CUI.

Although contract requirements for CUI have been in place since 2017, a May 2022 report from the Government Accountability Office (GAO) found at the time that the Department of Defense (DoD) was not fully compliant with CUI requirements across four areas, including categorizing Department CUI systems accurately and implementing the CMMC's 110 security requirements.¹ A subsequent DoD Inspector General audit report released on June 1, 2023, confirmed that "[a]lthough the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]) established CUI guidance, DoD Components did not effectively oversee the implementation of that guidance to ensure that CUI documents and e-mails contained the required markings and that DoD and contractor personnel completed the appropriate CUI training."² Without addressing the underlying CUI program, the current inconsistent marking process will continue to lead to increased costs and burdens on industry and degraded security for Department information.

- **2024 Cyber Survey:** The top challenges identified in NDIA's 2024 Cyber Survey include:
 - Financial cost associated with implementing NIST SP 800-171 (65.17%);
 - Insufficient guidance on NIST SP 800-171 compliance (45.51%);
 - Difficulty in understanding the security requirements in NIST SP 800-171 (38.2%); and
 - Shortage of qualified IT professionals (38.2%)

¹ U.S. Government Accountability Office. Protecting Controlled Unclassified Information Systems. May 2022. <https://www.gao.gov/assets/gao-22-105259-highlights.pdf>.

² U.S. Department of Defense, Office of the Inspector General. Audit of DoD's Implementation and Oversight of the Controlled Unclassified Information Program. DODIG-2023-078. June 1, 2023. <https://www.dodig.mil/reports.html/Article/3413433/audit-of-the-dodsimplementation-and-oversight-of-the-controlled-unclassified-i/>

In relation to the initial costs of implementing the 110 security requirements specified in NIST SP 800-171, nearly half of all the Cyber Survey respondents have spent more than \$100,000, 27.5% have spent more than a half million, nearly 12% have spent more than \$2 million, and nearly 5% have spent more than \$5 million in non-recurring costs to bring their systems into compliance.

Additionally, for the annual costs of maintaining these security requirements, over 45 percent of the respondents spend more than \$100,000, 20% spend more than one-half million, 11% spend more than \$2 million, and over 5% spend more than \$5 million dollars every year. So even after the initial setup costs, companies are on the hook for a substantial sum of resources to stay in compliance with the security requirements. It is expected that these costs will continue to increase as the ecosystem moves to NIST SP 800-171, Revision 3. Although the ordinary and necessary costs to meet NIST SP 800-171 are generally allowable costs, it does become a competitive decision for small businesses that may have fewer contracts to spread out the costs of compliance.

It is also interesting to note from the Cyber Survey that over 21% of the respondents have less than 1 full-time equivalent employee who manages or supports IT for the organization, and over 31% of the respondents have less than 1 full-time equivalent employee who manages or supports the organization's cybersecurity efforts. Despite the challenges of complying with Department cybersecurity standards, many organizations do not have a full-time person on staff to even manage these efforts.

2. Which specific security controls has your organization found to deliver the most tangible uplift of cybersecurity and actual risk reduction?

Although not an exhaustive list, NDIA member companies have highlighted the following security controls as the most beneficial:

- Multi-factor authentication
- Patch management (flaw remediation)
- Access control
- Endpoint detection and response
- Security awareness and phishing training
- Timely patching and vulnerability management
- Email filtering and anti-phishing

3. Conversely, which specific regulatory requirements or security controls create the highest administrative overhead and financial burden with the least measurable improvement to your actual cybersecurity posture?

Although not an exhaustive list, NDIA member companies have highlighted the following security controls as the least beneficial:

- Maintaining logs of physical access
- CUI identification and over-scoping
- Control CUI posted or processed on publicly accessible systems

- Excessive documentation requirements
- Media marking and accountability
- Comprehensive System Security Plan maintenance
- Rigid configuration baseline & change control management
- Excessive assessment and plan of action & milestones (POA&M) documentation

4. Describe how your organization utilizes existing commercial cybersecurity capabilities, platforms, managed services, or any other additional strategies or initiatives to safeguard data, improve operational resiliency, and reduce cybersecurity risk, and how the DoW might better recognize or accept these commercial solutions within a compliance or risk framework.

- NDIA member companies routinely utilize third-party services as part of their IT and cybersecurity ecosystem, including FedRAMP-authorized cloud enclaves and Security-as-a-Service (SaaS) platforms, cloud service providers (CSPs), managed service providers (MSPs), and managed security service providers (MSSPs), among others. Member companies have highlighted that eliminating the requirements for FIPS and FedRAMP would greatly expand the available options.

Additionally, as FedRAMP continues to evolve into FedRAMP 20x, the Department should work with the FedRAMP 20x program to harmonize terminology going forward. Defense contractors have historically sought out FedRAMP Moderate providers, knowing that using these capabilities provided some level of protection for CUI. With the FedRAMP program retiring the term “Moderate,” the FAR (and DFARS) will need to be updated to reflect this change and align terminology to ensure contractors continue to procure the level of protections the government demands, while ensuring that compliance nomenclature reflects the level of protection needed to offer protections for CUI.

5. Regarding Phase I self-assessments, what specific administrative or technical challenges does your organization face in maintaining, verifying, and reporting compliance, and how could this process be fundamentally streamlined? Have your self-assessments led to a more dynamic cyber posture approach, or are they performed only for compliance purposes?

- Member companies report that documentation is by far the most time-consuming and burdensome aspect of self-assessment, with the least impact on actual cybersecurity. As mentioned before, the over-scoping and/or under-scoping of CUI and federal contract information can be a costly challenge for industry.

6. What specific, actionable, policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically reduce costs and barriers to entry for small, medium, and non-traditional businesses without degrading the protection of federal data?

- The Department should engage in a formalized process with industry and across the federal government to establish clear, consistent CUI identification and marking guidance. Additionally,

the Department should educate contracting officers and provide mechanisms for prime contractors to limit the unnecessary flow-down of CUI to protect their supply chains from the need to meet Level 2 CMMC requirements.

- Congress should analyze directing the U.S. National Archives and Records Administration to streamline and simplify onerous CUI marking requirements, and instead require that a CUI marking must be handled in accordance with CUI requirements to re-focus CUI expenditure on securing IT systems, rather than on non-value-added, onerous markings.
- Congress and the Department must work to enact provisions that support companies unable to adequately invest in cybersecurity protections, including tax credits and Small Business Administration (SBA) guaranteed loans. This could include support for Section 1626 of the Senate version of the Fiscal Year (FY) 2027 National Defense Authorization Act, which is currently under consideration, that proposes to establish a grant program where certain small businesses and new entrants could apply to receive up to \$100,000 to offset the cost of the Level 2 CMMC assessments conducted by Certified Third-Party Assessment Organizations (C3PAOs).

Attachment 1: Consolidated Response from NDIA’s San Diego Chapter

Respondent Profile and Method

The findings below are drawn from a structured survey of NDIA San Diego members conducted in late July and early August 2026. Forty-eight member organizations responded. The instrument used fixed-choice questions to allow clean aggregation and one optional open comment field. Percentages are the share of the 48 respondents selecting a given option; multi-select items sum to more than 100 percent. Where we quote a member, the quotation is anonymized and offered only to illustrate a pattern already visible in the aggregate data.

Who responded. The sample is small-business heavy and squarely within the population the RFI targets: 73 percent employ fewer than 50 people. By role, 54 percent identified as subcontractors or suppliers, 44 percent as professional or technical services firms, and 40 percent as primes (many respondents wear more than one hat); 12 percent identified as non-traditional entrants and 12 percent as cybersecurity service providers, MSP/MSSPs, or C3PAOs. Respondents span the full compliance journey, from not yet started (15 percent) to a completed Level 2 C3PAO assessment (roughly one in six).

The Central Finding: Strong Support for the Goal, Strong Rejection of the Current Mechanism

Member sentiment	% (n=48)
Protecting DoD information in the supply chain is a necessary objective — agree	92%
The cost of compliance is proportionate to the risk it actually reduces — disagree	69%
The requirements are clear enough to know when a company is compliant — disagree	69%
The CMMC program requires change (major overhaul 50% + targeted reform 44%)	94%
The program is working as intended and needs no change	6%

This split is the through-line of every answer that follows. Members are not asking to be relieved of the duty to protect federal information. They are asking for that duty to be defined clearly, scoped to real risk, and implemented in a way a company of ten or thirty people can actually execute. We note honestly that the membership is divided on how far reform should go — a near-even split between “major overhaul” and “targeted reform” — and that a minority, concentrated among assessment professionals, cautions against weakening independent verification. We address that dissent in the closing section rather than bury it.

RFI Question 1 — Top prohibitive cost drivers, administrative burdens, and operational challenges

Members were asked to select their top five cost drivers and, separately, the operational effects of implementation. The results identify assessment, cloud migration, and documentation labor as the dominant costs, and identify lost business and diverted leadership attention as the dominant operational harms.

Most-cited cost drivers (top 5 permitted)	% (n=48)
C3PAO assessment fees	58%
Migration to GCC High or another government cloud	52%
Internal staff hours spent on documentation and evidence	48%
Consultant, RPO, or gap-assessment fees	46%
Hiring IT or security staff	40%
Recurring annual maintenance, affirmation, and evidence upkeep	33%

The burden is felt as disproportionate, not merely large. Reported total spend to date clusters in the tens to low hundreds of thousands of dollars rather than in extreme figures — but that is precisely the point for a small firm. Sixty percent of respondents reported spending at least one and a half times what they expected, a third spent more than double, and 17 percent stopped their compliance effort before they finished. As one member put it, the cost “pushes our rates into non-competitive territory,” and for pre-revenue entrants there is “no way to price it in” while staying competitive on already-thin margins.

The heaviest operational harms are business and organizational, not technical. Asked for the effects of implementation, members most often cited day-to-day productivity loss from added access friction (54 percent) and leadership time pulled away from running the business (48 percent) — an acute cost in firms where the owner is also the compliance lead. Inconsistent

prime interpretation (42 percent) and data-exchange friction with primes and teammates (40 percent) point to a coordination failure across the supply chain, not just a per-company cost. One in three reported IT or security staff burnout or turnover.

The most consequential burden is the one that never appears on an invoice: lost participation. Across the effects question, 44 percent of respondents reported taking at least one market-contracting action — declining or no-bidding DoD work (27 percent), considering exit from the defense market entirely (27 percent), or shifting revenue focus toward commercial or non-DoD work (23 percent). This is the industrial-base contraction the Task Force was convened to arrest, measured directly.

“As a pre-revenue new entrant, the biggest impact isn’t the cost of an assessment — it’s the go/no-go decision made before any bid exists. The companies you’re losing aren’t the ones leaving; they’re the ones that never arrive.”

RFI Question 2 — Controls that deliver the most tangible security uplift

Members were clear about what works, and the answer is instructive: the highest-value controls are widely available commercial security practices, not CMMC-specific artifacts. This finding directly informs Questions 3 and 4.

Controls cited as delivering real security value (top 5 permitted)	% (n=48)
Multifactor authentication	79%
Security awareness and phishing training	52%
Timely patching and vulnerability management	42%
Endpoint detection and response (EDR/XDR)	31%
Email filtering and anti-phishing	27%

The concentration at the top matters. Multifactor authentication was named by nearly four in five respondents; the leading practices overall are the same controls a well-run commercial firm already deploys, and are available as native features of mainstream platforms. The chapter’s recommendation follows from this directly: a reformed program should orient around a compact core of demonstrably high-value controls, and should recognize that most members can already meet that core using commercial capabilities they own today (see Question 4).

RFI Question 3 — Requirements with high overhead and least measurable security benefit

The signal here is precise and important: members did not report that the technical safeguards are worthless. They reported that the apparatus surrounding those safeguards — CUI identification, scoping, evidence documentation, and interpretation — generates the most cost for the least security return. Only half of respondents felt implementation made them meaningfully more secure at all; 38 percent reported no meaningful security change despite significant cost and effort.

CUI identification and over-scoping is the single most-cited source of low-value burden, appearing both as the hardest requirement to interpret (46 percent) and as the dominant theme of the open comments. Members describe requirements flowed down onto work with no plausible CUI nexus at all.

“I often see RFPs requiring CMMC certification even though no part of the project contains anything that should be CUI — changing exit signage in a dormitory; a fire-extinguisher pump house. No CUI is provided and none is stored.”

“Painting, coating, repairing a broken window, installing ceiling tile or bathroom tile should not require Level 2. These are examples of excessive flowdown, because CUI cannot be deconstructed.”

Beyond CUI identification, the requirements members found hardest to interpret — our proxy for high administrative overhead with contested value — were External Service Provider and shared-responsibility boundaries (38 percent), control of CUI flow under 3.1.3 (38 percent), and the content, format, and sufficiency of the SSP and POA&M (35 percent). Documentation and evidence upkeep recurs throughout: members ask that meeting a technical requirement be treated as evidence of meeting it, rather than requiring a separate documentary artifact for each objective. The recommendation is not to delete controls wholesale, but to (a) fix CUI identification at the source, (b) publish binding plain-language interpretations of the contested objectives, and (c) reduce evidence formalism where the technical control is verifiable directly.

RFI Question 4 — Use of commercial capabilities, and how DoW might recognize them

Members already rely heavily on commercial and government-community platforms, and they show strong appetite for models that let the government recognize or furnish those capabilities rather than requiring each small firm to build and certify its own environment.

Commercial / community capabilities already in use	% (n=48)
Microsoft 365 GCC or GCC High	42%
Microsoft 365 commercial with security add-ons	29%
A CMMC-focused enclave or compliant-workspace product	29%
AWS, Azure, or another FedRAMP-authorized cloud	27%
MSP or MSSP with 24/7 monitoring	23%

Asked which alternative delivery models they would seriously consider, members endorsed government-furnished and government-recognized options at high rates — and only 17 percent rejected a government-provided environment outright.

Alternative delivery models members would consider	% (n=48)
A DoW-hosted environment contractors subscribe to that stores/processes CUI (Flankspeed-style)	52%
Government-furnished laptops or virtual desktops issued for CUI work	52%
Direct subsidy, grant, or allowable-cost treatment for small-business compliance spend	44%
Government-negotiated enterprise (bulk) pricing for GCC High and comparable platforms	38%
A government-vetted catalog of pre-certified commercial environments conferring presumptive compliance	31%

Recommendation. The Department should recognize commercial and community capabilities in three concrete ways. First, grant presumptive compliance for the controls a vetted platform already satisfies — inheritance rather than re-proof — via a published, government-maintained catalog. Second, stand up or extend a government-hosted CUI environment that contractors can subscribe to, modeled on the Navy’s Flankspeed and the Army’s emerging NCODE, and exempt work performed wholly within it from separate certification. Third, use the government’s buying power to negotiate enterprise pricing for the compliant platforms small firms are already forced to buy individually. Half of our members would use a hosted government environment; the critical design requirement, raised explicitly by members, is that doing CUI work inside it must remove the member’s own systems from assessment scope — otherwise it adds cost rather than removing it.

RFI Question 5 — Self-assessment challenges, and whether it drives a dynamic posture

Members report that self-assessment, as currently structured, functions more as a periodic paperwork exercise than as a driver of continuous security — and that its central problem is evidentiary uncertainty and the absence of any feedback loop.

Reported self-assessment / SPRS challenges	% (n=48)
Uncertain what evidence we would need to defend our score	54%
Scoring methodology is confusing or counterintuitive	48%
Our self-assessment is primarily a compliance exercise, not a security driver	42%
We get no feedback — we submit and hear nothing	42%
Concerned about personal or corporate liability for the affirmation	35%

Only 21 percent said their self-assessment genuinely drives their security program. Members observe a structural mismatch, articulated well by one respondent: a static, cyclical audit that samples fixed evidence cannot keep pace with a cyber environment where change is “ongoing and elusive.” The reform members ask for is not the elimination of self-assessment but its redesign — clear evidence standards published in advance, a comprehensible scoring model, an actual feedback loop from the Department, and a shift toward lighter-weight, more continuous verification. On liability, one in three cited exposure under the affirmation as a live concern; a defined safe harbor for good-faith, documented effort would materially reduce it.

RFI Question 6 — Actionable reforms to reduce cost and barriers to entry for small, medium, and non-traditional businesses

Asked to select the reforms they most want, members prioritized clarity of scope, proportionality, and relief from universal third-party certification — in that order.

Most-wanted reforms (top 5 permitted)	% (n=48)
Resolve what qualifies as CUI definitively, at the contract level, before award	52%
Allow Level 2 self-assessment with risk-based government verification (vs. universal C3PAO)	48%
Offer a government-hosted CUI environment and exempt subscribers from separate certification	42%
Provide direct cost offset — grants, tax credits, or allowable-cost treatment	42%
Tier requirements by contract value, data sensitivity, or actual risk	35%
Reduce the 110 controls to a defensible core set	35%
Cap or standardize C3PAO fees and expand assessor capacity	35%

The chapter’s consolidated recommendation to the Task Force, drawn directly from these priorities:

- **Fix CUI at the source.** Require the contracting activity to make a definitive, contract-level CUI determination before award, and prohibit reflexive marking and flowdown of material with no CUI nexus. This is the highest-leverage single reform in the data; it is the root cause of over-scoping, excessive flowdown, and most interpretive cost.
- **Tier the requirement to the risk.** Establish a risk-based structure — including a micro-entity tier for the smallest firms — rather than a single uniform bar, so that a low-sensitivity, low-value effort does not carry the same certification weight as a high-sensitivity program.
- **Right-size verification.** Permit Level 2 self-assessment with risk-based government verification for lower-risk scopes, reserving mandatory third-party certification for higher-risk work. Pair any self-attestation path with a good-faith safe harbor and clear evidence standards.
- **Recognize and furnish infrastructure.** Stand up subscribable government-hosted CUI environments, grant control inheritance from vetted commercial platforms, and negotiate bulk platform pricing (see Question 4).
- **Make the cost recoverable and the systems fewer.** Deliver meaningful cost offset (grants, tax credits, or reliable allowable-cost treatment) and consolidate the proliferation of federal portals — SPRS, PIEE, DD-2345, CMMC, and bidding systems — that members describe as independently overwhelming.

RFI Question 7 — Actionable reforms to improve operational resilience against cyber attack

Because members identify the highest security value in a compact set of commercial controls, the most direct path to resilience is to concentrate attention and resources there rather than diffusing them across documentation.

- **Anchor the program to a high-value core.** Center requirements on the controls members found most effective — multifactor authentication, security-awareness training, timely patching, endpoint detection and response, and email defense — and reduce evidence formalism around lower-value objectives so that scarce small-business attention flows to the controls that actually reduce risk.
- **Shift from static audit to continuous assurance.** Members warn that a periodic, evidence-sampling audit cannot track a dynamic threat environment. Favor machine-readable, automatable verification (for example, OSCAL-based reporting and platform telemetry) over point-in-time manual review, which improves both resilience and assessment economics.
- **Reduce supply-chain fragility from inconsistency.** Standardize prime flowdown language and prohibit over-flowdown. Inconsistent interpretation across primes (cited by 42 percent) is itself a resilience problem: it wastes remediation effort and leaves genuine gaps unaddressed while firms chase contradictory guidance.
- **Fund capability where it is thinnest.** Government-sponsored cybersecurity and CUI-management workshops, mentoring, and shared secure infrastructure for the smallest firms would raise the true security floor of the base far more efficiently than requiring each micro-entity to reconstruct enterprise capability alone.

Feasibility, Member Division, and Risks — as required by the RFI format

Feasibility. The chapter deliberately weighted its recommendations toward measures achievable inside the Task Force’s 60-day window. Definitive CUI determination, standardized flowdown, published interpretations, a vetted platform-inheritance catalog, and extension of an already-operating government environment (Flankspeed) to contractors are policy and guidance actions, not multi-year technology builds. Tiering and self-assessment pathways can be implemented through acquisition policy. Cost-offset mechanisms are the most involved and would require coordination with acquisition and budget authorities.

Member division, represented honestly. This response reflects a clear majority, but not unanimity, and the Task Force should weigh the dissent. A vocal minority — concentrated among MSP/MSSP and C3PAO members and among small firms that have already certified — cautioned against weakening independent verification. Their arguments, in their words: self-attestation invites inflated scores, with affirming officials “giving themselves 110 with little to no evidence”; independent assessment “is essential to keep organizations honest because many are not”; the False Claims Act is a weak deterrent because it forces insiders to risk their careers to report; and one member stated flatly that the cost complaints are “significantly inflated.” A separate strand argued the real barrier is leadership culture and accountability rather than cost, and that proper scoping and budgeting can bring a Level 2 in for well under six figures. Still others urged the opposite of relief — stronger enforcement — noting that lax or deferred enforcement and acceptance of self-certification unfairly penalize the small businesses that did undertake the expense of full compliance in good faith.

Principal risks. The chapter flags three. First, any expanded self-assessment pathway must be paired with credible verification, evidence standards, and a safe harbor, or it will erode both security and the competitive position of firms that certified honestly — a fairness concern our own members raised pointedly. Second, resolving CUI must not devolve into a slower or more contested pre-award process; it should be a clear determination made by the contracting activity, not a new burden shifted onto industry. Third, tiering must be drawn on genuine risk, not solely on company size, so that a small firm handling genuinely sensitive information is not under-protected. The chapter offers these not as objections but as design constraints that make reform durable.

Closing. NDIA San Diego thanks the Task Force for opening this review to the companies that carry the program’s cost. Our members want to protect the Department’s information; they are telling you they need that duty defined clearly, scoped to real risk, and made affordable enough that the small and non-traditional firms the Department depends on can stay in the fight. We are glad to provide further detail or participate in follow-on engagement.