Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com
DUNS: 623799264d

July 26, 2026

Subject: Reforming CMMC and Reducing Compliance Burden for the DIB

To: Leanne Condren <leanne.m.condren.civ@mail.mil>

Dear Ms. Condren:

Thank you for the opportunity to comment on the reform of CMMC and in particular reducing the compliance burden for small and medium business subcontractors ("SMBs") in the Defense Industrial Base ("DIB"). TNE is an information consulting firm specializing in helping members of the DIB, especially SMBs, meet their contractual security requirements. Our comments herein address the issues we encounter most often in our work.

In our opinion, educating contract officers and pressuring prime contractors to end the unnecessary flow down of Controlled Unclassified Information ("CUI") would instantly reduce the number of SMBs requiring implementation of NIST SP 800-171. Primes routinely use document templates with default markings without reviewing whether the content of the document itself warrants those markings, and often these documents must be shared with Tier 2 and beyond. Vigilance in this regard would remove a tremendous compliance burden from the supply chain and give more SMBs the opportunity to meet only CMMC L1.

With respect to CMMC Level 1, we believe that the actual requirements of the FAR *Basic Safeguarding Rule* for protecting Federal Contract Information (FCI) were greatly expanded over the original intent of the rule via the CMMC Assessment Guide for Level 1. The very title of this rule, "*Basic Safeguarding*," makes it clear that the authors intended to enumerate basic things that businesses were likely already doing to protect their own proprietary data. However, CMMC complicated the implementation of this rule when the assessment objectives of NIST SP 800-171a were applied to the 15 requirements of the FAR. The 171a Assessment Guide was written for the application of advanced controls on a mature information security system. It is unreasonable to expect SMBs to apply these mature processes to their very simple systems.

In our opinion, the single most important reform for CMMC L1 would be to remove the assessment objectives for L1 and allow the FAR *Basic Safeguarding Rule* to stand on its own, as originally intended. By far the largest segment of the DIB will only need to achieve CMMC L1 compliance, especially if the flowdown of CUI is restricted, and this change would make that much, much easier for SMBs to do.

Conversely, in cases where CUI is present and protection is necessary, real advances in cyber security in the DIB were being made under CMMC. When DFARS 252.204-7012 took effect in 2016, we had a handful of SMBs reach out to us for assistance the first year, then none. When the interim rule took effect in 2020, the number of calls increased exponentially. When CMMC 1.0 was paused for review in 2021, the calls stopped again. When 32 CFR 170 was published, the floodgates opened. We have seen tremendous, immediate improvements in cyber security in the DIB each time the government took steps to enforce implementation.

Self-assessment doesn't work; the threats of DIBCAC and the FCA are ineffective. Only pre-award requirement for independent verification will force SMBs to implement the requirements in circumstances where they are warranted. Within hours of the announcement that the requirement for C3PAO assessment was being suspended, one client with whom we had been working since January to implement NIST SP 800-171 in their organization sent me a simple email halting all work. I have heard numerous stories in this vein from colleagues.

Perfection is a tough standard to achieve. The greatest bottleneck is not assessors (over 1000 available!) but rather SMB readiness. Eliminating C3PAO assessments would negatively impact cyber security in the DIB; however, reducing the minimum score required for Conditional L2 status and increasing the time allowed to close POAMs would greatly ease the burden, while continuing to improve cyber security in the DIB.

Respectfully submitted,

Glenda R. Snodgrass, President
grs@theneteffect.com

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com
DUNS: 623799264

Note: Our responses below are amalgamated from our experience assisting members of the DIB meet contract requirements.

Request for Information for Department of War

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.

- Poor or absent markings and the unnecessary flow down of Controlled Unclassified Information ("CUI") is by far the biggest challenge our SMB clients face.
- Requiring FIPS-validated encryption eliminates many affordable SMB tools from operating environments.
- Requiring FedRAMP Moderate or Equivalent for assets that process, store or transmit CUI limits available options and greatly increases the expense for SMBs. Note that this requirement did not come from NIST under its mandate to develop controls to protect CUI, but rather from DFARS 252.204-7012. There is no mention of FedRAMP in NIST SP 800-171 *"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."*
- Maintaining logs of physical access is extremely burdensome and expensive for SMBs, who routinely do not have anything in place to achieve this. Signing in and out on a clipboard when moving from one room to another throughout the day is tedious and time-consuming, while buying an automated system to meet this control is expensive. This requirement adds very little to overall security in the world of SMBs (where everyone knows everyone) and should definitely not be a requirement for the protection of FCI at CMMC L1.
- The implied requirements for documentation throughout 171 and 171a are extremely difficult, burdensome and expensive for SMBs. This standard could be lowered.

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

- Multi factor authentication
- Patch management (flaw remediation)
- Principle of least privilege

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?

- *"Maintain logs of physical access."*

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com
DUNS: 623799264

- *"Control CUI posted or processed on publicly accessible systems."* This control is a solution to a problem that doesn't exist. The assessment objectives require a rigorous procedure that is extremely difficult for SMBs to implement, and truly the likelihood of FCI or CUI accidentally being posted on a website or social media account is infinitesimal. That function is generally far removed from the FCI/CUI environment, even in SMBs.
- Overall, the excessive documentation requirements throughout 171 are extremely burdensome, and the direct correlation between documentation and effective cyber security in SMBs is tenuous at best.

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.

- Eliminating the requirements for FIPS and FedRAMP would greatly expand the available options.

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?

- Documentation is by far the most time-consuming and burdensome aspect of self-assessment, with the least impact on actual cyber security.
- The expectation of perfect and immediate compliance with 320 assessment objectives is unreasonable and discouraging to those who are trying.

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?

- Educate contract officers and pressure prime contractors to limit flowdown of CUI to protect their supply chains from the need to meet CMMC L2 requirements.
- Eliminate the assessment objectives for L1 and let the FAR *Basic Safeguarding Rule* stand on its own.
- Eliminate the FIPS validation requirement.
- Eliminate the FedRAMP requirement.
- Lower the minimum score for a Conditional L2 status, with a longer time frame for closing POAMs and achieving full compliance

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com
DUNS: 623799264

7. What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically improve operational resilience against cyber attacks at your organization?

- Reinstate the requirement for C3PAO assessment for contractors that truly need to protect CUI. This requirement has created the single biggest improvement in the level of cyber security in the DIB.
- Lower the minimum score for a Conditional L2 status, with a longer time frame for closing POAMs and achieving full compliance.
- Eliminate FIPS and FedRAMP requirements to permit the use of more affordable commercial products
- Encourage the use of MFA and patch management.