REQUEST-1

Request. **(a)** Allow CMMC-certified organizations and Government solicitations a six-month *period of time* to incorporate the changes in CMMC brought on when NIST SP 800-171r3 is made final, and **(b)** do not require any of the NIST SP 800-171r3 changes in CMMC certification assessments until six-months after NIST SP 800-171r3 is made final.

Justification. The date that NIST SP 800-171r3 will be made final has not yet been released. Many Organizations Seeking Certification (OSC) have implemented and are operationalizing their CMMC programs based on NIST SP 800-171r2, and many contracting officers are crafting solicitations based on "revision 2". To require compliance with "revision 3" on the date it is made final could negatively impact Government's procurement plans and unfairly hinder an OSC's ability to pass their assessment if they've implemented and are operationalizing CMMC in good faith based on "revision 2".

REQUEST-2

Request. As part of CMMC's impact on the acquisition process, require all solicitations that require the proposing organizations to self-attest their CMMC level to provide in their proposal proof of current *cyber liability insurance for first and third party damages* and make having this same insurance a requirement for contract award on the date of award in addition to signing the cybersecurity-compliance affirmation page.

Justification. The current CMMC program allows companies to self-attest their compliance with CMMC Level 1 (and possibly Level 2/Tier-1). The lack of the Government's insight into the legitimacy of such self-attestation should be seen as a risk. One way to mitigate negative impacts of this risk is to require such companies provide proof of cyber liability insurance for first and third party damages. Though the Government has recourse to prosecute any such companies that may be untruthful, this doesn't obviate any cybercrimes/damages incurred as the result of a company's lack of compliance; the cyber insurance will at least help mitigate such damages. Additionally, requiring cyber liability insurance encourages companies to prioritize cybersecurity measures. It incentivizes them to implement robust security controls and safeguards to mitigate the risk of cyber incidents and fosters a culture of continuous improvement.

REQUEST-3

Request. Allow/require C3PAOs to perform self-attestation cyber-hygiene reviews of companies selected as the potential awardee for a contract that requires CMMC self-attestation. Make this review part of the Government's potential-awardee-verification due-diligence.

Justification. The current CMMC program allows companies to self-attest their compliance with CMMC Level 1 (and possibly Level 2/Tier-1). The lack of the Government's insight into the legitimacy coupled with the Government's personnel limitations to "police" the legitimacy of self-attestations puts the Government at risk. One way to mitigate negative impacts of this risk is to use a CMMC-expert resource the Government has/is created/ing: its C3PAOs. The Government wouldn't have to hire new employees and/or train existing staff (already stretched thin) on CMMC self-attestation compliance/conformance.

REQUEST-4

Request. Allow an organization to recoup the costs associated with complying with DFARS 252.204-7012 and CMMC if it **(a)** affirms – in writing & signed by an officer of the company – that it has never been awarded a contract requiring such compliance obligation, and (b) is awarded a contract requiring 252.204-7012. Such cost-recuperation may be an evaluation

consideration for award, but should not be weighted as more important than technical considerations/solutions.
Justification. Where compliance has been required in the past, legally binding self-attestation and certification have not. The costs associated with such compliance are not insignificant and should not be a hinderance to the Government's access to the innovation, products and services that it deems necessary.

REQUEST-5
Request. Provide DoD-Acquisition/Procurement-tailored CMMC training to Government Acquisition & Procurement professionals (including legal & technical/functional managers) through the Defense Acquisition University (DAU) and industry partners. Initial in-depth training and refresher training on a regular basis and/or when CMMC-related regulations or requirements change should be required.
Justification. Most Government personnel that are involved in the acquisition & procurement lifecycle do not have an actionable understanding of CMMC to know how or where it should be applied to/in a solicitation. This introduces a significant risk to Government contracting since the failure to convey all of the CMMC requirements could result in awarding a contract to an unqualified contractor and/or delays in the acquisition/procurement process as errors are identified, all of which leads to delays in award, frustrated professionals, and delays or lack of mission support. The requirement for such CMMC training is supported by and described in the 2013 joint White Paper from the DoD and GSA to the President.

REQUEST-6
Request. Limit the CMMC levels to Level 1, Level 2, and Level 3 (remove the 2-tiers of Level 2). And, require organizations with CMMC Level 2 to both (i) undergo and pass a C3PAO audit/assessment every three (3) years, and (ii) conduct an annual internal audit/assessment and submit an annual self-attestation letter to the Government the each year not covered by the C3PAO audit/assessment.
Justification. Per the DOD, *CMMC is a culture shift* for Government and industry necessitated due to the increasingly more frequent cyber threats, attacks, and crimes targeting the Defense Industrial Base and need to protect and ensure national security. CMMC Level 1 requires organizations to annually self-attest their compliance with 17 specific NIST SP 800-171 security controls. Yet, CMMC Level 2 requires organizations to either (a) annually self-attest their compliance with all 110 of the NIST SP 800-171's security controls, or (b) undergo and pass a C3PAO audit/assessment every three years if they handle critical Government data pertaining to national security. Requiring and relying on the annual self-attestation of an organization that it is compliant with all 110 security controls introduces a significant risk to the Government; non-compliance (fibbing even just a little) is (a) absolutely possible given the current unchecked nature of self-attestation, and (b) highly probably for the same reason. Whether CUI is aligned to national security or not should not split the importance of protecting the Government's CUI; it has been categorized as CUI for a reason and those reasons should require the equal protection of the information. Additionally, splitting CMMC Level 2 will further confuse a community that is not yet trained or educated on the nuances of CMMC.