Date: October 10, 2023

From: Amira Armond, Kieri Solutions; Ryan Bonner, DEFCERT; and Matthew Carson, DEFCERT

To: Regulatory Information Service Center
1800 F Street, NW
Washington, DC 20405

Subject: *Scheduled E.O. 12866 Meeting 0790-AL49, Cybersecurity Maturity Model Certification (CMMC) Program*

The purpose of this letter is to provide feedback on the Cybersecurity Maturity Model Certification (CMMC) Program from the perspective of cybersecurity assessors who will be asked to judge solutions, as well as cybersecurity practitioners who are trying to assist defense contractors to comply.

Why CMMC is urgently needed

The CMMC program addresses a critical problem in defense procurement – that defense contractors who perform their cybersecurity responsibilities in accordance with DFARS 252.204-7012 are at a competitive disadvantage compared to peers that falsely attest to their compliance.

Contractors incur significant expense by implementing a security program compliant with DFARS 252.204-7012. This cost is incorporated into their bids for defense contracts, which makes those bids non-competitive compared to peers who have not implemented cybersecurity. Since the introduction of DFARS 252.204-7012, we believe that this core problem has driven compliant contractors from the market, reducing the number of defense contractors who are conscientious about their cybersecurity responsibilities.

In fact, even today, four years after the announcement of the CMMC program, defense contractors who incorporate cybersecurity costs into their bids are *still* at a competitive disadvantage compared to insecure peers. This will not be fixed until all contracts include a pre-bid requirement for third-party validation of DFARS 252.204-7012 compliance.

Recommendations:

Prioritize validated scores over perfect scores: As we have seen from the DIBCAC High Confidence assessments, a third-party validated score, even if low, is a better sign of compliance than a higher self-reported score. Very few defense contractors will be able to perfectly satisfy all requirements of NIST SP 800-171 in the next few years. In order to reduce risk to DoD operations resulting from reducing the number of eligible suppliers, the DoD would be better served by ensuring that submitted cybersecurity scores are accurate and validated. As such, defense contractors should be considered eligible for award only on the basis of having submitted a score to SPRS that has been validated by the DIBCAC, the responsible Program Manager (using a cybersecurity professional of their choice), or an accredited C3PAO. A time-bound Plan of Action and Milestones (POA&M) should be required for score submission. This will ensure the DoD is able to verify the submitted scores are accurate and determine the risk associated with open POA&M items in order to make informed decisions for awards while maintaining a grace period for defense contractors to complete the implementation of their cybersecurity programs as they continue to provide critical services and products to the government.

Encourage improvement: Drafts of the CMMC Assessment Process have included language which made perfect implementation of all "3-point" and "5-point" practices mandatory, even for an interim CMMC certificate. While we understand that the CMMC Assessment Process is not part of the DoD's official guidance, we are concerned that it may reflect the DoD's intentions for the CMMC program. Contractors should be allowed to fix any practice and quickly get re-assessed on just the failed practices, rather than being forced to start over with a new assessment. Being forced to start over is unduly punitive and will result in attrition of small manufacturers from the defense industrial base rather than encourage improvement.

Expedite rollout of CMMC to all defense contracts. CMMC assessor capacity is currently limited by demand. Demand is low because defense contractors incur a competitive disadvantage if they perform cybersecurity for contracts that do not include a third-part assessment requirement. By rolling out CMMC with a ramp-up initiative as described above, assessment organizations will be able to hire and pay for staff, reaching necessary capacity within 2 years. Picking-and-choosing contracts for CMMC will result in a much slower capacity build because CMMC Third Party Assessment Organizations (C3PAOs) cannot plan for a specific demand.

Weight compliance higher than price. In other words, bidders who are compliant with CMMC should be preferred over bidders who are not compliant with CMMC and are lower priced. DoD OUSD should offer guidance on how to weigh evaluation factors and prioritize third-party validated cybersecurity over Lowest Price Technical Acceptable (LPTA) criteria. If the DoD provides CMMC waivers to lowest-price bidders, despite higher-price bids with CMMC certificates, they will perpetuate the original problem which CMMC is intended to solve.

Accreditation Body oversight of CMMC assessment organizations

We believe that organizations, rather than individual Lead Assessors, should be responsible for the quality of assessments. A C3PAO promotes standardization of assessment and professional practices through centralized processes and management.

The original plan for an accreditation of C3PAOs by a DoD-approved Accreditation Body is important to the long-term health of the CMMC program.

Assessment organizations need to be validated to ensure they have processes for handling incidents appropriately; staff are qualified and professional; potential conflicts of interest are identified and remediated; and assessment records are quality reviewed and retained. If C3PAO performance is not held to a high standard by an accreditation body, third-party validation of cybersecurity will be influenced by market pressure to be less and less stringent. Bid protests will occur if CMMC assessments are tainted by conflicts of interest or obvious inconsistencies. These risks are best mitigated by an accreditation program.

To be clear, this is not a critique of the Cyber Accreditation Body. This is intended to re-iterate how important having an Accreditation Body, and the performance of accreditation assessments of C3PAOs, is to the long-term health of the CMMC program.

Recommendations:

Model the private-public partnership for CMMC assessments on the FedRAMP program. The Accreditation Body for FedRAMP uses a 14-page document (Assessment Guidance) which provides a simple framework for FedRAMP assessments. Detailed process and competence to perform assessment are verified by A2LA during their assessment of the 3PAO. If this model was used with the CMMC program, it would give assessors flexibility to validate a wide variety of environments and technologies. The CMMC C3PAO accreditation assessment would include a thorough review of

C3PAO procedures, review of incidents and staff capability, and sampling of assessment performance. The C3PAO's ability to perform high quality assessments would be ensured by the accreditation assessment.

Resist the urge to regulate specific staff training or individual assessor certification requirements into the 48 CFR or 32 CFR. The accreditation process and active quality management by C3PAO leadership is a more effective way to ensure that CMMC assessments are done with high quality.

Security requirements should protect CUI

We are concerned that the CMMC program will unintentionally require assessment of systems which are unrelated to the security of CUI.

Recommendations:

All scoping of security requirements should be directly tied to the protection of CUI. Guidance on scoping needs to include instructions that security requirements should only apply to components or systems if applying the requirement will contribute to the protection of CUI.

Assets that do not store, process, or transmit CUI should be assessed against a requirement only when failing to meet the requirement creates a risk of unauthorized CUI disclosure. This language should be written into the scoping guide.

The CMMC program should not stipulate requirements for External Service Providers unless the provider has the capability to affect the security of CUI by either 1) having direct possession of CUI, or 2) having access to or managing access to a CUI environment. If the CMMC program does stipulate requirements for External Service Providers, the requirement should be applied to information systems that affect the confidentiality of client CUI (by having access to CUI environments, by managing access to CUI environments, or by possessing CUI), not to provider organizations as a whole.

Untested mandate

If the official guidance for CMMC is updated during this rulemaking process, the risk of introducing requirements which conflict with each other, or which combine in unexpected ways, is very high. As assessors, we have already seen this in practice with the CMMC Level 2 Scoping Guide. We are concerned that DoD guidance will inadvertently result in situations where only contractors utilizing an entirely on-premises and self-hosted information system will be able to pass assessment. If problematic guidance is codified in 32 CFR and 48 CFR, a rule change will be needed to fix it, which will delay the CMMC program further.

Recommendations:

Minimize the amount of complexity in the CFR and instead assign responsibility to DoD CIO to provide guidance using a method that can be easily updated over time. In particular, the following topics are high-risk for unexpected assessment results and should be kept separate from the CFR:

- Requirements for external service providers (including CMMC or FedRAMP)
- Defining in-scope or out-of-scope assets
- Requirements for security systems
- Reciprocity for other cybersecurity frameworks

- Specific cybersecurity requirements or practices
- Instructions on how to perform an assessment
- Any references to NIST SP 800-171 which automatically increment as new revisions are published

Dependency on Service Providers

In our experience, the majority of defense contractors use at least one non-cloud service provider. If the CMMC program establishes certification requirements for those service providers, the program will experience delays because it will not be possible to certify the service providers, nor their clients, until after the rule is in effect.

Recommendation:

Avoid language in 32 CFR and 48 CFR which requires CMMC certification for service providers. Instead, allow C3PAOs to perform NIST SP 800-171 assessments of service providers prior to the CMMC program. Then, when performing CMMC assessments of defense contractors, allow audit reports from the NIST SP 800-171 assessments to be used as evidence that service provider information systems are protecting CUI at appropriate levels.

Certification does not validate shared services

Neither FedRAMP nor CMMC verify that a provider is protecting a defense contractor's information system. They only verify that a provider is protecting their own information system.

In order for CMMC to scale, shared services from service providers need to be assessed-once, inherited-many. For example, if a Managed Security Services Provider offers audit management as a service, it should be possible to assess the service once, verify it meets specific requirements related to audit management, then give credit for those requirements to all clients of the service.

Recommendations:

Explicitly allow C3PAOs to perform assessments of service providers which validate the performance of shared services. Reports from these assessments should be usable as standalone evidence for specific requirements by defense contractors. This avoids costs related to re-assessing the same service provider repeatedly for each of their clients.

Don't force assessors to accept irrelevant FedRAMP or CMMC certificates from service providers instead of verifying shared services.

Don't force service providers to get irrelevant FedRAMP or CMMC certificates if their information system cannot impact the confidentiality of CUI.

Thank you for your consideration -

Sincerely,

V. Amira Armond

Certified CMMC Assessor, Provisional Instructor, CISSP, CISA

President, Kieri Solutions

Ryan Bonner

Certified CMMC Assessor, Provisional Instructor

President, DEFCERT

Matthew Carson

Technical Compliance Consultant, DEFCERT