MEMORANDUM FOR SERVICE ACQUISITION EXECUTIVES  
COMPONENT ACQUISITION EXECUTIVES  

AUG 04 2020

SUBJECT: Implementing the Cybersecurity Maturity Model Certification within the Department of Defense

The Department of Defense released Cybersecurity Maturity Model Certification (CMMC) version 1.0 on January 31, 2020. The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references. Additionally, it encompasses the basic safeguarding requirements specified in the Federal Acquisition Regulation clause 52.204-21 and the security requirements for Controlled Unclassified Information (CUI) specified in the National Institute of Standards and Technology Special Publication 800-171 per the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012. The current version of the model and additional information is available at the CMMC website (www.acq.osd.mil/cmmc).

My office recently submitted a proposed change to the DFARS which is proceeding through the Office of Management and Budget rulemaking process. To facilitate a smooth transition of this new requirement across the Department, I am providing the following implementation guidance.

I am implementing CMMC using a phased-in approach. For FY 2021, I intend to limit the number of solicitations specifying a CMMC requirement to no more than 15 prime contracts, which will be CMMC pilot program efforts. Pursuant to this approach, I direct all Program Managers and Contracting Officers to avoid including CMMC as a requirement in Requests for Information and Requests for Proposals unless coordinated through the nomination process set forth in this memorandum.

To support the pilot program and initial implementation, I request the following:

- Each Service Acquisition Executive nominate three acquisitions with an expected contract award date in FY 2021.
- Each Component Acquisition Executive nominate a single acquisition with an expected contract award date in FY 2021.
- Each nomination should be for a mid-sized program that require the contractor to process or store basic CUI. This requirement aligns to CMMC level three.
• Do not nominate acquisitions that are solely for provision of commercial-off-the-shelf products, or for operational technology systems supporting industrial or manufacturing operations.

• Please submit your nominations to my point of contact, Ms. Stacy Bostjanick, at stacy.s.bostjanick.civ@mail.mil no later than August 15, 2020.

For subsequent fiscal years, the Department intends to incorporate CMMC Levels 4 and 5 while increasing the quantity of acquisitions that include a CMMC requirement. The phase in targets are:

• Year 2: 75 new acquisitions
• Year 3: 250 new acquisitions
• Year 4: 325 new acquisitions
• Year 5: 475 new acquisitions
• Year 6 and beyond: All new acquisitions and other transactions issued under authority of section 2371(b) of title 10, United States Code.

The Department is committed to working with our Defense Industrial Base partners to mitigate cybersecurity threats that target our supply chain and seek to undercut our technological advantages. The CMMC framework represents a key step to enhance the protection of intellectual property and sensitive unclassified information. If you have any questions regarding the CMMC implementation, please contact the Chief Information Security Officer for Acquisition, Ms. Katie Arrington, at katherine.e.arrington.civ@mail.mil or (703) 695-9332.

[Signature]
Ellen M. Lord