The purpose of this notice is to clarify DLA's planned implementation of Cybersecurity Maturity Model Certification Requirements (DFARS clause 252.204-7021) as directed by Interim Rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements. This notice is for informational purposes, addresses only the CMMC portion of Interim Rule 2019-D041, and should not be interpreted as directive, all-encompassing, or a deviation from Department of Defense (DoD) policy.

DLA will implement CMMC requirements in accordance with the subject rule and subsequent direction from the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)). Accordingly, **beginning on 1 October 2025**, CMMC will apply to all DLA solicitations and contract actions, including those for the acquisition of commercial items (except those exclusively "Commercial Off The Shelf (COTS)" items) valued at greater than the micro-purchase threshold.

Additionally, OUSD(A&S) directed a phased implementation of CMMC beginning in FY21 through full implementation in FY26. DLA expects to identify Pilot acquisitions (acquisitions that include the CMMC via 252.204-7021) in the following quantities:

- FY21: 1 new acquisition
- FY22: 5 new acquisitions
- FY23: 17 new acquisitions
- FY24: 22 new acquisitions
- FY25: 32 new acquisitions

The above numbers are estimates based on DoD-wide targets and are subject to change. Additionally, DLA may, if the acquisition warrants and with OUSD(A&S) approval, include CMMC requirements on acquisitions in excess of the above targets.

Industry partners are advised to monitor solicitations for DFARS clause 252.204-7021 to ensure compliance with CMMC requirements when warranted. Until full CMMC implementation, DLA will make every effort to articulate clearly when CMMC requirements apply to an acquisition. If there are questions regarding application of CMMC requirements to a specific acquisition, consult with the contract specialist.

For more information on CMMC, as well as other DoD cybersecurity initiatives, Project Spectrum is a recommended resource (https://projectspectrum.io). Project Spectrum is supported by the DoD Office of Small Business Programs, and provides information, training, and risk assessments to help vendors improve cyber readiness and comply with DoD requirements. Additionally, the Procurement Technical Assistance Centers (PTACs) provide vendors free assistance, including assistance related to DoD cybersecurity initiatives, to help them pursue contracts from DLA and other federal agencies. For more information refer to - https://www.dla.mil/SmallBusiness/PTAP/

NOTE: The provision at DFARS 252.204-7019, "Notice of NIST SP 800-171 DoD Assessment Requirements," implements a related rule requiring certain vendors to conduct a NIST SP 800–171 self-assessment (also referred to as a basic assessment) and post their score in the Supplier Performance Risk System (SPRS). **The rule in DFARS 252.204-7019 was effective on Nov 30, 2020 and is related, but different, than DoD/DLA's implementation of CMMC.** Refer to the Nov 30, 2020 DIBBS notice for more - https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=1048