



ACQUISITION
AND SUSTAINMENT

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

MEMORANDUM FOR COMMANDER, UNITED STATES CYBER
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES SPECIAL OPERATIONS
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION
COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY
(PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY
(PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE
(CONTRACTING)
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Interim Defense Federal Acquisition Regulation Supplement Rule, 2019-D041,
Assessing Contractor Implementation of Cybersecurity Requirements

The purpose of this memorandum is to ensure workforce awareness and understanding of the requirements of interim Defense Federal Acquisition Regulation Supplement (DFARS) rule, 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, which was published in the Federal Register (85 FR 61505) on September 29, 2020, and is effective on November 30, 2020.

The interim rule implements the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The interim rule requires contracting officers to take specific actions prior to awarding contracts, task or delivery orders, or exercising an option period or extending the period of performance, on or after November 30, 2020. The executive summary (Attachment 1) provides an overview of the interim DFARS rule, and the Under Secretary of Defense for Acquisition and Sustainment memorandum, dated August 4, 2020, (Attachment 2) implements CMMC within the Department.

My point of contact is Lt Col Bryan Lamb, who is available by phone at 703-693-0497, or by email at bryan.d.lamb.mil@mail.mil.

TENAGLIA.
JOHN.M.11
54945926

Digitally signed by
TENAGLIA.JOHN.M.
1154945926
Date: 2020.11.25
12:21:07 -05'00'

John M. Tenaglia
Principal Director,
Defense Pricing and Contracting

Attachments:
As stated

EXECUTIVE SUMMARY
**INTERIM DFARS RULE, 2019-D041, ASSESSING CONTRACTOR IMPLEMENTATION OF
CYBERSECURITY REQUIREMENTS**

- DoD published the interim DFARS rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, on September 29, 2020, with an effective date of November 30, 2020.
 - o The interim rule implements the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) framework, and requires contracting officers to take specific actions prior to awarding contracts, task or delivery orders, or exercising an option period or extending the period of performance, on and after November 30, 2020.
 - o In accordance with FAR 13.201(d), neither the CMMC nor the NIST SP 800-171 DoD Assessment requirements are required for purchases at or below the micro-purchase threshold. FAR 13.201(d) reads as follows: “Micro-purchases do not require provisions or clauses, except as provided at 13.202 and 32.1110. This paragraph takes precedence over any other FAR requirement to the contrary, but does not prohibit the use of any clause.” The interim rule did not add to the clause identified at DFARS 232.1110, and therefore does not impose requirements for micro-purchases.
- **NIST SP 800-171 DoD Assessment:** On or after November 30, 2020, the contracting officer shall, prior to awarding a contract, task order, or delivery order to, or exercising an option period or period of performance with, an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at DFARS 252.204-7012, verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) is posted in Supplier Performance Risk System (SPRS) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order.
 - o Contracting officers should refer to DFARS PGI 204.7303 for additional information on Safeguarding Covered Defense Information and Cyber Incident Reporting requirements.
 - o The requiring activity is responsible for identifying aspects of the contract requirement that involve operationally critical support or covered defense information, and that have the potential for generation or use of covered defense information during the period of performance. However, contracting officers should understand these terms as defined in DFARS Clause 252.204-7012, and be familiar with the CUI categories described in the Controlled Unclassified Information (CUI) Registry.
- **CMMC:** On or after November 30, 2020, when a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not award to an offeror that does not have a CMMC certificate at the level required by the solicitation, or exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract. Contracting officers shall use Supplier Performance Risk System (SPRS) to verify an offeror or contractor’s CMMC level.
 - o To implement a phased rollout, CMMC requirements will apply only to certain new contracts, task orders, or delivery orders awarded from November 30, 2020, through September 30, 2025. During this time period, inclusion of a CMMC requirement must be approved by the Undersecretary of Defense for Acquisition and Sustainment (USD(A&S)).

- o The USD(A&S) memorandum, “Implementing the Cybersecurity Maturity Model Certification within the Department of Defense,” dated August 4, 2020, details the phased application of CMMC beginning intended for no more than 15 prime contracts in Fiscal Year 2021 as CMMC pilot program efforts.
- o On or after October 01, 2025, CMMC requirements will apply to all solicitations and contracts or task orders or delivery orders, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items.
- o The CMMC level to be required for subcontractors is the level that is appropriate for the information that is being flowed down to the subcontractor.
- **DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.**
On or after November 30, 2020, use the new provision at DFARS 252.204-7019 in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.
- **DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.**
On or after November 30, 2020, use the new clause at DFARS 252.204-7020 in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items. This clause is required to be flowed down to subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).
- **DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements.**
Inclusion of the clause at DFARS 252.204-7021 will be phased in according to the dates below:
 - o November 30, 2020, through September 30, 2025, use the new clause at DFARS 252.204-7021 in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items, if the requirement document or statement of work, as determined by the requiring activity and approved by OUSD(A&S), requires a contractor to have a specific CMMC level.
 - o In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation, prior to September 30, 2025, must be approved by OUSD(A&S).
 - o On or after October 1, 2025, use the clause at DFARS 252.204-7021 in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.
 - o This clause is required to be flowed down to all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding COTS items.

Relevant URLs:

- Link to Interim DFARS Rule 2019-D041, Federal Register Notice:
<https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf>
- Link to Interim DFARS Rule 2019-D041, DFARS Text:
[https://www.acq.osd.mil/dpap/dars/dfars/changenotice/2020/20200929/2019-D041%20\(i\)%20DFARS%20Text%20LILLO.docx](https://www.acq.osd.mil/dpap/dars/dfars/changenotice/2020/20200929/2019-D041%20(i)%20DFARS%20Text%20LILLO.docx)
- Supplier Performance Risk System (SPRS)
<https://www.sprs.csd.disa.mil/>
- National Archives - Controlled Unclassified Information (CUI) Registry
<https://www.archives.gov/cui/registry/category-list.html>

ACQUISITION
AND SUSTAINMENT

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

AUG 04 2020

MEMORANDUM FOR SERVICE ACQUISITION EXECUTIVES
COMPONENT ACQUISITION EXECUTIVES

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:

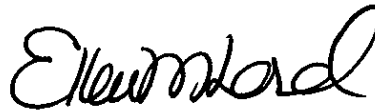
- Each Service Acquisition Executive nominate three acquisitions with an expected contract award date in FY 2021.
- Each Component Acquisition Executive nominate a single acquisition with an expected contract award date in FY 2021.
- Each nomination should be for a mid-sized program that require the 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.



Ellen M. Lord