National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology

The NIST SP 800-171 DoD Assessment Methodology is one of two cybersecurity assessment methodologies addressed in DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, published in Federal Register, 85 Fed. Reg. 61505 (Sep 29, 2020), and effective Nov 30, 2020 **(see flipside of this document for second methodology)**. The interim rule will be followed by future rulemaking that may amend rule content and requirements. Public comments (due Nov 30, 2020) will be considered in formulation of final rule.

The NIST SP 800-171 DoD Assessment Methodology builds on DFARS 252.204-7008 requirement for Offerors to represent they will implement NIST SP 800-171 security requirements, as required by DFARS 252.204-7012, by providing for assessment of a contractor's implementation of the NIST SP 800-171 security requirements.

DFARS Amendments to Implement the NIST SP 800-171 DoD Assessment Methodology

DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting:

- Directs contracting officers to verify summary level score of a current (not older than three years unless a lesser time is specified in the solicitation) NIST SP 800-171 DoD Assessment for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order is posted in the Supplier Performance Risk System (SPRS), prior to:
  - Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 pursuant to the clause at DFARS 252.204-7012, or;
  - Exercising option period, or extending period of performance on contract, task order, or delivery order, with contractor required to implement NIST SP 800-171 pursuant to DFARS 252.204-7012.
- Directs contracting officers to include DFARS 252.204-7019 and DFARS 252.204-7020 in all solicitations and contracts except those solely for the acquisition of commercially available off-the-shelf (COTS) items.

DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements:

- Prescribed for use in all solicitations, except for solicitations solely for the acquisition of COTS items. DoD does not intend to apply clause at or below micro-purchase threshold.
- Notifies offerors that, if the offeror is required to implement NIST SP 800-171, the offeror must have a current (not older than three years unless a lesser time is specified in the solicitation) NIST SP 800-171 DoD Assessment for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order to be considered for award.
- Offerors must verify summary level scores of current NIST SP 800-171 DoD Assessment are posted in SPRS.

DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements:

- Prescribed for use in all solicitations and contracts, task orders, or delivery orders, except those solely for acquisition of COTS items. DoD does not intend to apply clause at or below micro-purchase threshold.
- Applicable to covered contractor information systems that are required to comply with NIST SP 800-171, in accordance with DFARS 252.204-7012.
- If applicable, requires the contractor to provide Government access to facilities, systems, and personnel necessary for DoD to conduct a Medium or High NIST SP 800-171 DoD Assessment.
- Requires the contractor to include the substance of the clause, in all subcontracts and other contractual instruments including subcontracts for commercial items but excluding COTS items.
- Contractor shall not award a subcontract or other contractual instrument that is subject to the implementation of NIST SP 800-171, in accordance with DFARS clause 252.204-7012, unless the subcontractor has completed at least a Basic NIST SP 800-171 DoD Assessment.

For more information on the NIST SP 800-171 DoD Assessment Methodology, go to the DPC Cyber page ***here.***

Cybersecurity Maturity Model Certification (CMMC) Framework

The CMMC Framework is one of two cybersecurity assessment methodologies addressed in DFARS Case 2019-D041 Assessing Contractor Implementation of Cybersecurity Requirements, published in the Federal Register, 85 Fed. Reg. 61505 (Sept. 29, 2020), and effective Nov 30, 2020 **(see flipside of this document for second methodology)**. The 2019-D041 interim rule will be followed by future rulemaking that may amend the rule content and requirements. Public comments are due on Nov 30, 2020 and will be considered in the formulation of a final rule.

The CMMC Framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a defense industrial base (DIB) contractor can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

DFARS Amendments to Implement the CMMC Framework

DFARS subpart 204.75, Cybersecurity Maturity Model Certification (CMMC):

- Directs contracting officers to include in the solicitation the required CMMC level and requires contractors to achieve, at time of award, a CMMC certificate at the level specified in the solicitation.
- Directs contracting officers to verify in the Supplier Performance Risk System (SPRS) that the successful offeror has achieved a CMMC certification that is current (i.e., not more than 3 years old) and meets the CMMC level required in the solicitation prior to making award

DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements:

- Until Sep 30, 2025, prescribed for use in all solicitations and contracts or task orders or delivery orders, including those for commercial items but excluding those solely for the acquisition of COTS items, **if the requirement document or statement of work requires a contractor to have a specific CMMC level, and inclusion of the CMMC requirement in the requirement document or statement of work has been approved by the Undersecretary of Defense for Acquisition and Sustainment (USD(A&S))**.
- On or after Oct 1, 2025, prescribed for use in all solicitations and contracts or task orders or delivery orders, including those for commercial items but excluding those solely for the acquisition of COTS items. DoD does not intend to the apply the clause at or below the micro-purchase threshold.
- Requires a contractor to have a current CMMC certificate at the CMMC level required by the contract, and maintain the CMMC certificate at the required level for the duration of the contract.
- Requires the contractor to include the substance of the clause, in all subcontracts and other contractual instruments, including those for the acquisition of commercial items, excluding COTS items.
- Requires the contractor, prior to awarding a subcontract or other contractual instrument, to ensure the subcontractor has a current CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

For more information on the CMMC Framework, go to the CMMC website at ***https://www.acq.osd.mil/cmmc/***