ROGERS JOSEPH O'DONNELL, PC

DFARS: ASSESSING CONTRACTOR IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS (DFARS CASE 2019-D041)

On September 29, 2020, the Defense Acquisition Regulations System, Department of Defense ("DoD") issued an interim rule to implement two distinct but related assessments of cybersecurity requirements: first, the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800–171 DoD Assessment Methodology and, second, the Cybersecurity Maturity Model Certification ("CMMC") Framework, "in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain" (the "Interim Rule"). DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61,505 (Sept. 29, 2020).

"The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by" Department of Defense Federal Acquisition Regulation Supplement ("DFARS") clause 252.204–7012," Safeguarding Covered Defense Information and Cyber Incident Reporting. *Id.* DFARS clause 252.204-7012 requires that contractors "apply the security requirements of NIST SP 800–171 to 'covered contractor information systems.'" *Id.* The assessment set forth in the NIST SP 800–171 DoD Assessment Methodology "uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment." *Id.*

The CMMC Framework builds upon the NIST SP 800–171 DoD Assessment Methodology by adding "a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level." *Id.* For each CMMC level, the associated sets of maturity processes and cybersecurity best practices, drawn from multiple references and standards, are cumulative and "demonstrate a progression of cybersecurity maturity." *Id.* at 61,505-06. In this regard, the CMMC Framework includes the basic requirements for safeguarding Federal Contract Information ("FCI") in Federal Acquisition Regulation ("FAR") clause 52.204–21, "Basic

Safeguarding of Covered Contractor Information Systems," as well as the more stringent security requirements for Controlled Unclassified Information ("CUI") in NIST SP 800–171, in accordance with DFARS clause 252.204–7012. *Id.* DoD intends to implement "a phased rollout of CMMC." Therefore, until September 30, 2025, the inclusion of a CMMC requirement in a solicitation must be approved by DoD's Office of the Under Secretary of Defense for Acquisition and Sustainment ("OUSD(A&S)"). CMMC will apply to all DoD solicitations and contracts, except those for commercially available off-the-shelf ("COTS") items, starting on or after October 1, 2025.

The Interim Rule will become effective on November 30, 2020. Comments submitted in writing by November 30, 2020 will be considered in the formation of the final rule.

The Implications of the Interim Rule for DoD Government Contractors, Government Contracts Clauses, and Government Personnel

A. Impact on DoD Government Contractors

The Interim Rule requires that DoD government contractors:

- Possess at least a Basic NIST SP 800-171 DoD Assessment that is not more than three years old at the time of award (if they are required to implement NIST SP 800-171). 85 Fed. Reg. 61,519 (DFARS 204.7302(a)(2)).
- Achieve a CMMC certificate at the level specified in a solicitation at the time of award and maintain a CMMC certificate at that level that is not more than 3 years old for the life of the contract, task order, or delivery order, if such certificate is required by the applicable statement work or requirement document. *Id.* at 61,520 (DFARS 204.7501 (b)).

B. Impact of the Interim Rule on DoD Government Contracts

The Interim Rule requires that DoD government contracts:

- Include a new DFARS provision (252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements) in all solicitations, except for those solely for the acquisition of COTS items. *Id.* at 61,519 (DFARS 204.7304(d)).

- New DFARS provision 252.204-7019, Notice Of NIST SP 800-171 DoD Assessment Requirements (NOV 2020):
  - Requires that an offeror (that is required to implement NIST SP 800-171) possess an assessment (that is not more than 3 years old) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order in order to be considered for award. *Id.* at 61,520 (DFARS 252.204-7019(b)).
  - Requires that an offeror verify that summary level scores of a NIST SP 800-171 DoD Assessment (that is not more than 3 years old) are posted in the Supplier Performance Risk System ("SPRS") for all covered contractor information systems relevant to its offer. *Id.* at 61,520-21 (DFARS 252.204-7019(c)(1)). The SPRS landing page is at https://www.sprs.csd.disa.mil/.
  - Allows an offeror to conduct and submit a Basic Assessment for posting to SPRS using a specified format, where an offeror does not have summary level scores of a NIST SP 800-171 DoD Assessment (that is not more than 3 years old) posted in SPRS. *Id.* at 61,521 (DFARS 252.204-7019(c)(2)).

- Include a new DFARS clause (252.204-7020, NIST SP 800-171, DoD Assessment Requirements) in all solicitations and contracts, task orders, or delivery orders, except for those that are solely for the acquisition of COTS items. 85 Fed. Reg. 61,519 (DFARS 204.7304(e)).
  - New DFARS clause 252.204-7020, NIST SP 800-171, DoD Assessment Requirements (NOV 2020):
    - Applies to covered contractor information systems that are required to comply with NIST SP 800-171 (in accordance with the DFARS clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting). *Id.* at 61,521 (DFARS 252.204-7020(b)).
    - Requires that certain contractors provide access to their facilities, systems, and personnel so that the government can conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in the NIST SP 800-171

DoD Assessment Methodology. *Id.* (DFARS 252.204-7020(c)). The current version of the DoD Assessment Methodology (v.1.2.1, June 24,2020) is available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

- Allows a contractor to submit summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171, DoD Assessment Methodology, for posting in SPRS. *Id.* at 61,522 (DFARS 252.204-7020(d)(1)).
- Provides that DoD will provide Medium and High Assessment summary level scores to a contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores in the SPRS. *Id.* (DFARS 252.204-7020(e)(1)).
- Provides a contractor with 14 business days to submit additional information to demonstrate that it meets any security requirements not observed by the assessment team or to rebut findings that may be in question. 85 Fed. Reg. 61,522 (DFARS 252.204-7020(e)(2)).
- Requires a contractor to insert DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements (NOV 2020), in all subcontracts and other contractual instruments, including for the acquisition of commercial items except for COTS items. *Id.* (DFARS 252.204-7020 (g)(1)).
- Requires that a contractor not award a subcontract or other contractual instrument unless the subcontractor has completed at least a Basic NIST SP 800-171 DoD Assessment for all covered contractor information systems relevant to its offer within the last 3 years. *Id.* (DFARS 252.204-7020(g)(2)).
- Allows a subcontractor that does not have summary level scores of a NIST SP 800-171 DoD Assessment that is not more than 3 years old to conduct

and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, for posting in the SPRS. *Id.* (DFARS 252.204-7020(g)(3)).

- Include, until September 30, 2025, new DFARS clause 252.204-7021, CMMC Requirements, in solicitations and contracts or task orders or delivery orders, except for those solely for the acquisition of COTS items, if:
  - the applicable requirement document or statement of work requires a contractor have a specific CMMC level; and
  - inclusion of that requirement has been approved by the OUSD(A&S). *Id.* at 61,520 (DFARS 204.7503(a)).
- Include, on or after October 1, 2025, new DFARS clause 252.204-7021, Contractor Compliance with CMMC Level Requirements, in all solicitations and contracts, task orders, or delivery orders, except for those solely for the acquisition of COTS items. *Id.* (DFARS 7503(b)).
  - New DFARS clause 252.204-7021, Contractor Compliance with the CMMC Level Requirements:
    - Requires that a contractor have a CMMC certificate at the CMMC level required by the applicable contract that is not older than 3 years and maintain a CMMC certificate at the required level for the duration of that contract. 85 Fed. Reg. 61,522 (DFARS 252.204-7021(b)).
    - Requires that a contractor insert the substance of new clause 252.204-7021, Contractor Compliance with the CMMC Level Requirements, in all subcontracts and other contractual instruments, excluding subcontracts for the acquisition of COTS items. *Id.* (DFARS 252.204-7021(c)(1)).
    - Requires that, prior to an award to a subcontractor, a contractor ensure that the subcontractor has a CMMC certificate at the level that is appropriate for the information that is being flowed down to the subcontractor that is not older than three years. *Id.* (DFARS 252.204-7021(c)(2)).

C. Impact on Government Personnel

The Interim Rule requires government personnel to:

- Conduct High NIST SP 800-171 DoD Assessments, using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. *Id.* at 61,519 (DFARS 204.7302(a)(4)).
- Verify that the summary level score of a NIST SP 800-171 DoD Assessment for each relevant covered contractor information system (and that is not more than 3 years old) is posted in SPRS before a contract, task order, or delivery order is awarded to or an option period is exercised on or the period of performance is extended on a contract, task order, or delivery order. *Id.* (DFARS 204.7303(b)).
- Include any CMMC level specified by the requiring activity in the relevant solicitation. 85 Fed. Reg. 61,520 (DFARS 204.7501(a)).
- Not award a contract, task order, or delivery order to or exercise an option period or extend the period of performance on a contract, task order or delivery order with a contractor that does not have a CMMC certificate at the level required by the solicitation, contract, task order, or delivery order that is not more than 3 years old. *Id.* (DFARS 204.7501(a) and (b)).
- Not award a contract to or exercise an option on or extend any period of performance on a contract, task order, or delivery order with a contractor that does not have a CMMC certificate at the level required by the solicitation or contract. *Id.* (DFARS 204.7502(a)).
- Use the SPRS to verify a contractor's CMMC level. *Id.* (DFARS 204.7502(b)).
- Exercise an option only after verification in the SPRS that the summary level score of a NIST SP 800-171 DoD Assessment (that is not more than 3 years old) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order is posted in the SPRS, and that a contractor possesses a CMMC certificate at the level required by the contract that is not more than three years old. *Id.* (DFARS 217.207(c)(2)).

D. Other Implications in the Preamble to the Interim Rule

1. New Contract Clauses and Provisions

- The Interim Rule's new contract clauses and provisions will apply to contracts and subcontracts for the acquisition of commercial items (except for COTS items) and to acquisitions valued at or below the simplified acquisition threshold, but greater than the micro-purchase threshold. *Id.* at 61,507.

2. NIST SP 800–171 DoD Assessment

- An offeror that is required to implement NIST SP 800–171 on covered contractor information systems pursuant to DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload its score in the SPRS. 85 Fed. Reg. 62,511.
    - A contractor that has fully implemented all 110 NIST SP 800–171 security requirements, will have a score of 110 to report in SPRS for their Basic Assessment. *Id.*
    - A contractor will use the scoring methodology to add up the value of any unimplemented requirements it has and subtract the total value from 110 to determine its Basic Assessment score. *Id.*
- After a contract is awarded, DoD may conduct a Medium or High Assessment of an offer based on how critical the program is or how sensitive the information being handled by the contractor is. *Id.* at 62,512.
    - Under both the Medium and High Assessment, DoD will review a contractor's description of how each NIST SP 800–171 security requirement is met and will identify any descriptions that do not properly address those security requirements. *Id.*

3. CMMC Framework

- A contractor may obtain a CMMC level for its entire enterprise network or a segment or enclave of its enterprise, depending on where the information to be protected is processed, stored, or transmitted. *Id.* at 61,505.
- CMMC Third Party Assessment Organizations (C3PAOs), accredited by an independent, nonprofit CMMC–Accreditation Body ("AB"), will conduct CMMC assessments and, upon completion of such assessments, the CMMC−AB will provide the contractor with a certification. 85 Fed. Reg. 61,506, 61,513.
- C3PAOs will provide CMMC Assessment reports to the CMMC–AB who will maintain and store these reports. *Id.* at 61,513.
- Contractors that do not process, store, or transmit CUI, must obtain a CMMC level 1 certification. *Id.* at 61,510.
    - CMMC Level 1 adds an on-site assessment from a C3PAO—to verify the implementation of required cybersecurity practices and bolster the physical identification of contractors and subcontractors in the DoD supply chain—to the requirements of FAR clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems. *Id.* at 61,516.
    - Under the CMMC Framework, a contractor may achieve a CMMC Level 1 certification if it can demonstrate implementation of the basic safeguarding requirements in FAR clause 52.204–21. *Id.* at 61,519.
- Contractors that process, store, or transmit CUI must achieve a CMMC level 3 or higher. *Id.* at 61,510.
    - A contractor may achieve a CMMC Level 3 certification under the CMMC Framework if they can demonstrate implementation of the NIST SP 800–171 security requirements, as well as certain additional processes and practices. 85 Fed. Reg. 61,519.
- A contractor will not be able to achieve compliance status using plans of action under the CMMC Framework. *Id.* at 61,509.

- If a contractor disputes a C3PAO assessment, that contractor may submit a dispute adjudication request to the CMMC–AB, as well as any supporting information. *Id.* at 61,513.
    - The CMMC–AB will use a formal process to review the contractor's adjudication request and provide a preliminary evaluation to the contractor and C3PAO. *Id.*
- If a contractor does not accept the CMMC–AB preliminary evaluation, that contractor may request an additional assessment by the CMMC–AB. *Id.*

E. Effective Date

- The Office of the Secretary of Defense will coordinate with military services and agencies to identify contracts that will include the CMMC requirement prior to October 1, 2025. *Id.* at 61,510.
- Although the Interim Rule incorporates a delayed effective date, it also encourages contractors and subcontractors (that are required to implement NIST SP 800-171, pursuant to DFARS clause 252.204−7012) to conduct and submit the self-assessment described in the Interim Rule immediately. 85 Fed. Reg. 61,518.

For information contact:

Robert S. Metzger | Shareholder
ROGERS JOSEPH O'DONNELL, PC
875 15th Street, N.W., Suite 725 | Washington, D.C. 20005
311 California Street, 10FL | San Francisco, CA 94104
202.777.8951 direct (DC) | 415.365.5355 direct (SF)
rmetzger@rjo.com | www.rjo.com | **LinkedIn**

Alexandria Tindall Webb | Of Counsel
ROGERS JOSEPH O'DONNELL, PC
875 15th Street, N.W., Suite 725 | Washington, D.C. 20005
202.777.8950 main | 202.777.8958 direct
ATindallWebb@rjo.com | www.rjo.com | LinkedIn

Deborah Norris Rodin | Associate
ROGERS JOSEPH O'DONNELL, PC
875 15th Street, N.W., Suite 725 | Washington, D.C. 20005
202.777.8950 main | 202.777.8959 direct
drodin@rjo.com | www.rjo.com | LinkedIn

Eleanor Ross | Associate
ROGERS JOSEPH O'DONNELL, PC
875 15th Street, N.W., Suite 725 | Washington, D.C. 20005
202.777.8950 main | 202.777.8957 direct
eross@rjo.com | www.rjo.com | LinkedIn