Raytheon Technologies
870 Winter Street
Waltham, MA 02451
USA

U.S. Government Subcontractor Regulatory Alert

Supply Chain Cybersecurity Compliance - DFARS Interim Rule Released 09-30-20
252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
252.204-7020, NIST SP 800-171 DoD Assessment Requirements
252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Please note, the following is for informational purposes only and not for purposes of providing legal advice. You should contact your attorney to obtain legal advice as needed.

This communication is to inform you of an interim rule (DFARS Case 2019-D041) – *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements*, the Department of Defense (DoD) published on September 30. The interim rule takes effect November 30, 2020 and will require immediate action by the DoD supply chain to be eligible to receive awards after the interim rule goes into effect.

Currently, pursuant to DFARS 252.204-7012, government suppliers must provide adequate security for covered contractor information systems. A "covered contractor information system" is defined as an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. More specifically, government suppliers must protect such information systems by implementing the security controls of National Institute of Standard and Technology (NIST) Special Publication (SP) 800-171.[1]

Beginning November 30, 2020, among other things, Contracting Officers must include the new DFARS 252.204-7019 provision and DFARS clause 252.204-7020 clause in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of commercial-off-the-shelf (COTS) items. These will require the DoD supply chain to quantify their current cybersecurity compliance with NIST SP 800-171 requirements using the NIST SP 800-171 DoD Assessment Methodology. **Pursuant to 252.204-7020, contractors such as RTX may not award a subcontract or other contractual instrument that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS 252.204-7012, unless the supplier has:**

1. **Completed *at least* a Basic Assessment in accordance with NIST SP 800-171 DoD Assessment Methodology (or in the alternative the Government performed Medium or High Assessment) within the last three years for all covered contractor information systems relevant to its offer that are not part of an information technology system operated on behalf of the Government; and**

2. **To the extent the supplier completed a Basic Assessment, it submitted its summary level scores, and other information required by paragraph (d) of DFARS 252.204-7020, either directly into the Supplier Performance Risk System (SPRS) or via encrypted email to webptsmh@navy.mil for posting to the SPRS.**

In addition, the contractor must insert the substance of DFARS 252.204-7020, including paragraph (g), in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.

[1] In accordance with NIST SP 800-171, suppliers should already be aware of the security requirements they have not yet implemented and have documented plans of actions for those requirements.

Accordingly, suppliers subject to this requirement should take the necessary steps for compliance and be prepared to provide RTX with a representation and certification of compliance upon request.

Overview of Interim Rule

The interim rule creates three new provisions and clauses:

- 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Together, they implement two cybersecurity initiatives, the: (1) Cybersecurity Maturity Model Certification (CMMC) framework and (2) NIST SP 800-171 DoD Assessment Requirements.

The DoD is implementing a systematic, phased rollout of the CMMC requirements over five years, after which, it will apply to all DoD procurements, except for certain acquisitions such as those that are solely for COTS items. In FY2021, the DoD is expected to identify only 10 to 15 programs that will require CMMC. To the extent CMMC applies, the solicitation will include the required CMMC level and DFARS 252.204-7021 will be incorporated in the applicable contract and subcontract(s). It requires contractors subject to the CMMC requirement to have and maintain a current third-party CMMC certificate issued at the CMMC level required by the contract, and prior to making an award to a subcontractor, to ensure that 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.

Beginning November 30, 2020, the DoD will implement its other initiative, the NIST SP 800-171 DoD Assessment Requirements through the new provisions DFARS 252.204-7019 and DFARS 252.204-7020. These provisions, and in particular, the impact of DFARS 252.204-7020 on supply chain, are discussed above in more detail.

Key Takeaways

To summarize and reinforce some important potential compliance impacts from the interim rule:

- Your company must immediately take steps to complete at least a Basic Assessment (or in the alternative, the Government has conducted a Medium or High Assessment) for all covered contractor systems relevant to your offer that are not part of an information system or service operated on behalf of the Government, and submit your company's summary level scores and other required information to SPRS if your company is subject to implementation of the NIST SP 800-171 security requirements in accordance with DFARS 252.204-7012.
- Contractors must insert the substance of DFARS 252.204-7020, including paragraph (g) titled "subcontracts," in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.
- It is important your company continue its CMMC readiness activities, be prepared to respond to inquiries regarding your CMMC readiness plan, and ensure that your suppliers are aware of the CMMC effort and encourage them to become educated on it.

Additional Information

- The USG's Supplier Performance Risk System (SPRS) can be accessed here
- Additional information on CMMC and a copy of the CMMC model can be found here
- The interim rule can be found here

Thank you for your support. If you have any questions regarding cybersecurity and the DFARS 252.204-7020 provision related to Raytheon Technologies or its business units, please e-mail supplier_cybersecurity@rtx.com.