New: Contractor Cybersecurity Requirements to effect primes, subs and suppliers

The Department of Defense issued an Interim Rule titled – Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041) on Tuesday, September 29, 2020.

The rule's effective date is November 30, 2020 and will likely affect current and future contractors interested in conducting business with the Department of Defense either as prime contractors or as a member of the Defense Industrial Base's supply chain when solicitations include DFARS 252.204-7012.

It was determined that "urgent and compelling reasons exist to promulgate this *Interim Rule* without prior opportunity for public comment." It was also noted that "Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security." As a result of this rule being issued as an *Interim Rule*, it is less likely that there will be substantive changes to the rule. Interested parties are invited to submit comments.

The issuing of this rule does not change either DFARS clause: 252.204-7008 or DFARS 252.204-7012. In addition to amending several sections of the DFARS, the rule also identifies five NAICS codes (541712, 236220, 541330, 541519 & 561210) expected to be impacted based upon award information and inclusion of DFARS clause 252.204-7012. The rule also adds the following three new clauses:

- 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
- 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Subcontracts – flow down: Yes)
- 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement (Subcontracts – flow down: Yes)

Section 204.7302(2) specifies that "contractors required to implement NIST SP 800-171, in accordance with the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7019).

Of these three clauses, current and prospective contractors need to review the first two clauses and take immediate action as required. The third clause addresses CMMC requirements.

The impact of 252.204-7019 is that contracting officers must verify current Summary DoD Assessment prior to awarding a contract or taking similar contractual actions detailed in the rule.

Clause 252.204-7020 is applicable to primes as it directs "The Contractor shall 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 clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment as described in https:/www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

Assistance with the new Cybersecurity requirement and implementation of new regulations, please contact Marc Violante, WPI's Director, Federal Market Strategies at marcv@wispro.org

Also, take a look at the continuing Cyber Friday's schedule on topics for Federal contractors and subcontractors SCHEDULE