

Supplier Cybersecurity

Beginning November 30, 2020, Contracting Officers must include the new DFARS 252.2047019 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 ARC Technology Solutions 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***

- 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
- 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.