



Northrop Grumman
2980 Fairview Park Drive
Falls Church, Virginia 22042-4511

northropgrumman.com

November 23, 2020

Subject: Supply Chain Cybersecurity Compliance Reminder – Action Required

Dear Valued Supply Chain Partner:

In follow-up to our [September 30th letter](#), we want to remind you of the importance of taking appropriate actions now to comply with new Interim Rule Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements ([DFARS Case 2019-D041](#)) going into effect on November 30, 2020. This rule requires suppliers other than COTS providers to have completed one of two cyber assessments – a basic NIST SP 800-171 self-assessment or a third party Cybersecurity Maturity Model Certification (CMMC) -- prior to award of any subcontract or purchase order that incorporates the applicable clauses.

Most contracts will **require your company to have a current NIST SP 800-171 Department of Defense (DoD) Assessment score (less than three years old) posted in the DoD's Supplier Performance Risk System (SPRS) for all covered contractor information systems subject to the current DFARS 252.204-7012 (i.e., systems that process Covered Defense Information)**. At a minimum, suppliers are required to conduct a basic self-assessment using the specified DoD weighted assessment methodology on each covered contractor system that will process Covered Defense Information (CDI) during contract performance to be eligible for contract award, and post the score and other specified data, including importantly a POAM date by which all 110 NIST SP 800-171 controls will be fully implemented to the [SPRS website](#), unless DoD has already conducted a medium or high confidence assessment of the system. This assessment requirement, based upon the [NIST SP 800-171 DoD Assessment Methodology](#), will be implemented through 2 new clauses DFARS 252.204-7019 and DFARS 252.204-7020 that will be in the majority of contracts over the next several years.

Some contracts alternatively will include DFARS 252.204-7021, which will require you to have a CMMC prior to award at the specified level of maturity. Please note that this rule applies to all suppliers (unless purely COTS) even if their systems do not process CDI. DoD will be implementing the CMMC program gradually over the next 5 years and does not intend to have CMMC applicable to all contracts until FY 2026. In FY2021, DoD is aiming to impose the third party CMMC certification model on 15 contracts/programs by

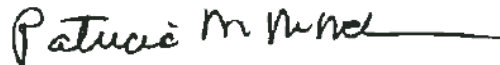
inserting new clause DFARS 252.204-7021 in its solicitations. It is our understanding that DoD intends to announce those opportunities that will be subject to CMMC in FY21 around the time the interim rule goes into effect.

- Additional information on CMMC and a copy of the CMMC model can be found at <https://www.acq.osd.mil/cmmc/index.html>.

As previously shared, the [CyberAssist](#) website includes Guides, Standards, Tools, and other resources as well as the practice descriptions for all five (5) levels of the CMMC Program to support you on your path to CMMC certification. You may also contact your Northrop Grumman procurement representative on questions regarding these requirements and other contractual issues.

We greatly appreciate your continued commitment to enhance the protection of information within the supply chain.

Sincerely,

A handwritten signature in black ink that reads "Patricia M. McMahon" followed by a horizontal line.

Patricia M. McMahon
Vice President, Corporate Supply Chain