

October 1, 2020

**Subject: Supply Chain Cybersecurity Compliance – DFARS Interim Rule Released**

Dear Valued Supply Chain Partner:

We wanted to alert you that the highly anticipated new Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)<sup>1</sup> was published on September 29th in the Federal Register as an interim rule, rather than as a proposed rule as was originally expected. The interim rule does not change any of the existing DFARS Cyber clauses, including DFARS 252.204-7012. It rather adds three new DFARS cyber clauses focused on assessing company's compliance with the applicable cybersecurity standard, whether that be Cybersecurity Maturity Model Certification (CMMC) or the existing requirement to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

We recommend that, in addition to continuing your CMMC readiness activities, your company review the interim rule closely and familiarize itself with NIST SP 800-171 Assessment Methodology<sup>2</sup>, so you can begin conducting your basic assessment of your systems that process CDI so that you be eligible to receive awards after the interim rule goes into effect.

The three new DFARS clauses added through this Interim Rule are:

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

The interim rule will go into effect on November 30th, 60 days from the Federal Register posting. The deadline for submitting comments on the interim rule will be that same day. The supplementary information provided with the interim rule confirms our understanding that CMMC will apply to only 10 to 15 programs in FY2021, and the program will continue to be rolled out until October 1, 2025, at which time it will apply to all DoD procurements. To the extent that an RFP specifies that CMMC will apply, the statement of work or other requirements will

---

<sup>1</sup> <https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>

<sup>2</sup> [https://www.acq.osd.mil/dpap/pdi/cyber/strategically\\_assessing\\_contractor\\_implementation\\_of\\_NIST\\_SP\\_800-171.html](https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html)

specify the necessary CMMC level and DFARS 252.204-7021 will be incorporated into the resulting contract or subcontract. The clause mandates that any system that will process Covered Defense Information (CDI) be certified at the specified CMMC level for a contractor or subcontractor to be eligible for award. The clause must be flowed down to subcontractors and suppliers if CDI will be processed by the companies. The interim rule does not provide any other information as to whether or how a lower CMMC maturity level could be permitted at lower tiers.

For the majority of the contracts issued in the next couple of years, DoD will continue to incorporate DFARS 252.204.7012, which requires companies to implement NIST SP 800-171 on any covered contractor information system that will process CDI. After the interim rule becomes effective, DoD will incorporate DFARS 252.204-7019 and DFARS 252.204-7020. Those clauses impose a requirement that companies conduct a basic self-assessment of their implementation of the 110 NIST 800-171 controls on relevant systems in accordance with the NIST SP 800-171 DoD Assessment Methodology released last year, and submit the resulting scores to DoD to be eligible for award of any DoD contract or subcontract subject to the interim rule. The new clauses also require companies to cooperate with any requests for DoD itself to conduct medium or high assessments.

- Additional information on CMMC and a copy of the CMMC model can be found at <https://www.acq.osd.mil/cmmc/index.html>.
- The NIST SP 800-171 DoD Assessment Methodology is available at [https://www.acq.osd.mil/dpap/pdi/cyber/strategically\\_assessing\\_contractor\\_implementation\\_of\\_NIST\\_SP\\_800-171.html](https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html).
  - The Assessment 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).
  - A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government.

As Hypatia previously announced, the CyberAssist website (<https://ndisac.org/dibsc/cyberassist/>) includes the practice descriptions for all five (5) levels of the Cybersecurity Maturity Model Certification (CMMC) Program to support you on your path to CMMC certification.

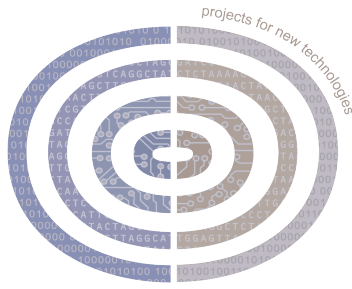
We value your continuous support, and, most importantly, we hope you and your employees are safe and healthy. Please do not hesitate to contact me directly with any questions at 301-651-6662 (cell) or 571-346-7612 (office).

Sincerely,



Kelly M. McVeary, Ph.D., M.A., Ed.M.  
Co-Founder and CEO

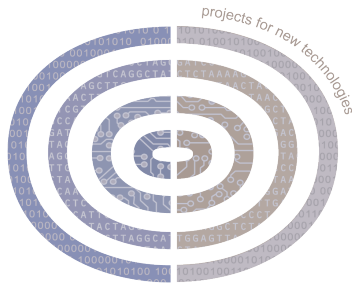
CC: Mrs. Margaret Molloy  
Mr. Brian Steel  
Dr. Stanley Fricke  
Laura Bushnell  
Suppliers



invest + research | design + build

# HYPATIA PROJECT





invest + research | design + build

# HYPATIA PROJECT

