



Cybersecurity Maturity Model Certification (CMMC)



- The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.
- The new standard and maturity model will be named Cybersecurity Maturity Model Certification (CMMC)
- The CMMC levels will range from basic hygiene to “State-of-the-Art” and will also capture both security control and the institutionalization of processes that enhance cybersecurity for DIB companies.
- The required CMMC level (notionally between 1 – 5) for a specific contract will be contained in the RFP sections L & M, and will be a “go/no-go decision”.
- The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.
- The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.
- The CMMC will include a center for cybersecurity education and training.
- The CMMC will include the development and deployment of a tool that 3rd party cybersecurity certifiers will use to conduct audits, collect metrics, and inform risk mitigation for the entire supply chain.