



Supplier Cybersecurity

Department of Defense – Cybersecurity Maturity Model Certification

In late January 2020, the Department of Defense released the Cybersecurity Maturity Model Certification (“CMMC”) Version 1.0. If you are a Rolls-Royce supplier that supports a DoD contract it is important that you understand the DoD’s cybersecurity initiative. The DoD is establishing the new CMMC framework to enhance the cybersecurity posture of the U.S. Defense Industrial Base (“DIB”). The CMMC is expected to be a verification process to ensure the DoD supply chain has appropriate levels of cybersecurity controls and processes in place to protect controlled unclassified information (“CUI”) that is maintained on contractors’ networks.

All companies that are part of the DIB must comply, not just those companies handling CUI. Contractors will no longer just self-attest to compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, but will be subject to 3rd party assessors that will independently review whether internal systems and processes used for DoD work have the required cybersecurity controls in place to comply with CMMC. The DoD plans to begin issuing a select number of solicitations in 2020 that will include the new requirement. While the DoD has rolled out this new requirement, full implementation is not expected until 2026. However, once a contractor receives a contract or subcontract with the CMMC requirements they are expected to be compliant.

CMMC levels cover a 1 to 5 range depending on a contractor’s level of cyber hygiene (basic to advanced). These requirements are expected to apply to all tiers of the DoD supply chain, including the supply of commercial items and commercial off the shelf (“COTS”) items, regardless of whether the supplier receives or develops CUI. You can find the requirements needed to achieve the five cybersecurity maturity levels within CMMC v.1.0.

The DoD created a CMMC website to provide guidance on the CMMC process and requirements to prepare for certification. Rolls-Royce encourages you to visit the [CMMC website](#) maintained by the Office of the Under Secretary of Defense for Acquisition & Sustainment to learn more and determine the impact on your business.

To begin your effort toward CMMC assessment, we recommend that you consider the following:

- 1) verifying that you are compliant with DFARS 252.204-7012 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 at a level that will be necessary for the CMMC assessment needed to support your business;
- 2) review the CMMC v.1.0 to determine any additional requirements and the next steps your business needs to take in order to prepare for a 3rd party assessment.