



Thursday, March 4, 2021

Subject: **Changes to DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting**

Dear Valued Supplier,

This letter is to inform you of new cybersecurity requirements recently announced by the US Department of Defense (DoD) which require suppliers in the DoD supply chain to take incremental compliance steps, these are effective on new contracts.

New cybersecurity requirements:

Three new interim rules have been published regarding cybersecurity, and took effect on November 30, 2020. These rules must be flowed down to lower -tier suppliers, and they extend the provisions of the original DFARS 252.204-7012 rule as follows:

DFARS 252.204-7019:

In order to be considered for an award containing DFARS 252.204-7012, a supplier must post (or have a current) summary compliance score on the DoD Supplier Performance Risk System (SPRS) system. The compliance score must be generated using the DCMA SP 800-171 assessment methodology, it must be less than 3 years old, and is considered a **Basic** Assessment if the supplier has generated the score using only their internal compliance reviews. Access to SPRS to load supplier compliance scores is made via the DoD PIEE Portal, although scores can also be submitted by email to webpmsmh@navy.mil. If a supplier has previously been subject to a DoD **Medium** or **High** Cybersecurity Assessment by DCMA, then a compliance score will have already been posted on the supplier's behalf).

DFARS 252.204-7020:

When present, this rule authorizes the DoD to validate a suppliers **Basic** Assessment score by progressively:

- (i) Performing a thorough review of all documents relating to the information system, including the suppliers own self-assessments; and engaging in direct discussion with the supplier to obtain clarifications and additional information. This increases the DoD's confidence in the supplier's self-assessed score to **Medium**.
- (ii) Additionally, performing verification, examination, and demonstration activity on the supplier's information system; to confirm that security requirements have been implemented as described. This increases the DoD's confidence in the supplier's self-assessed score to **High**.

This means that the supplier, if required, must permit DoD agencies to access it's physical facilities, it's information systems and assessment artefacts, and it's personnel.

DFARS 252.204-7021:

When present, this rule requires the supplier to have a current (less than 3 years old) Cybersecurity Maturity Model Certification, provided by an assessor licensed by the CMMC Accreditation Body.

Required supplier actions:

Supplier compliance with NIST SP 800-171, is already mandated by DFARS 252.204-7012. However, by introducing DFARS 252.204-7019 and DFARS 252.204-7020, DoD is aiming (with effect from Nov 30th 2020) to verify the status of a supplier's compliance; and Electromech Technologies is prohibited from awarding new contracts subject to DFARS 252.204-7012 to a supplier that does not have a current score posted on SPRS. Therefore:

1. Unless DCMA has already conducted a **Medium** or **High** level assessment of your information system, please complete a **Basic** self-assessment using the DCMA SP 800-171 assessment methodology.
2. Post this assessment score to the Supplier Performance Risk System (SPRS) system either via PIEE or by email, as soon as possible.




3. Tell Electromech Technologies that you have completed steps 1 and 2, and provide a copy of your SPRS posting.

By publishing DFARS 252.204-7021, DoD has confirmed how it intends to flow the requirements of the Cybersecurity Maturity Model Certification into future contracts. DoD will phase-in CMMC on new contracts over the next 5 years. Electromech Technologies is prohibited from awarding new contracts subject to DFARS 252.204-7021, to a supplier that does not have a current CMMC certificate. Therefore:

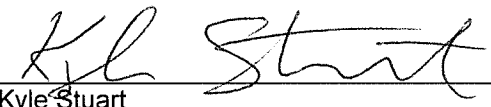
4. Suppliers should review the readiness of their information systems, against the requirements of the Cybersecurity Maturity Model Certification specification (CMMC v1.02). (Suppliers who collect, develop, receive, transmit, use or store CDI should prepare to achieve at least Level 3 certification).

It is important that your company is able to validate your ongoing compliance with DFARS 252.204-7012, as required by DFARS 252.204-7019, and DFARS 252.204-7020; and that you are preparing for CMMC certification as required by DFARS 252.204-7021. Please also ensure that your own lower-tier suppliers are also aware of these changes, and encourage them to become educated on them.

If you have any questions regarding cybersecurity and these new DFARS, please reach out to your local procurement representative or e-mail etpurchasing@electromech.com



Mauricio de la Serna
Electromech Technologies
VP of Operations



Kyle Stuart
Electromech Technologies
VP of Engineering