Notice to Suppliers

Upcoming CMMC Webinar

Originator: Neil Brink
Job Title: Supply Chain Cybersecurity
Business Unit: Defence

NTS Number: 567
Issue: 1
Date: 1 March 2023

Scope/Applicability:
All Rolls-Royce suppliers with US Department of Defense (DoD) subcontracts

Dear Supply Partner,

Introduction:

While the details related to CMMC (Cybersecurity Maturity Model Certification) are still working their way through the rulemaking process, Rolls-Royce and MxD, National Center for Cybersecurity in Manufacturing, are hosting a webinar to clarify what you need to know about the updated requirements and how to prepare for compliance.
Please join us for the ***Comply with CMMC in 2023*** webinar on March 22.

What is CMMC?
The DoD Cybersecurity Maturity Model Certification (CMMC) is a future requirement for DoD contractors who process, store, develop, or transmit DoD controlled unclassified information (CUI). The DoD has implemented several changes to the program since its original release in 2020, however the current notice of proposed rulemaking is expected in May 2023.

Why Should I Care?
CMMC will require most contractors in the DoD supply chain to obtain a third-party or self-certification of their compliance with stated cybersecurity controls. It is anticipated that NIST SP 800-171 will remain the base requirements set for CMMC Level 2 requirements, similar to the current Defense Federal Acquisition Regulation Supplement. (DFARS). The biggest differences between the DFARS and CMMC programs is:

- the requirement for a third-party audit
- the requirement for full compliance to NIST SP 800-171 at the point of assessment

DFARS vs. CMMC?
Under the current DFARS provision 252.204-7019 and DFARS clause 252.204-7020, DoD contractors may self-assess using the DoD Assessment Methodology. The proposed CMMC requirements for organizations who process, store or transmit critical CUI will need a triennial assessment performed by a Certified 3rd Party Assessment Organization (C3PAO). For many organizations, the shift from self-assessment to third-party assessment holds the greatest risk as documented evidence of compliance to the requirements will need to be available and inspectable by the C3PAO to achieve a successful audit.

MxD and RR are here to answer your questions and provide assessment tools to prepare you for these changes. Join us for this webinar where we will break down the latest on CMMC, DFARS and other DoD cyber requirements:

Register now for the Comply with CMMC 2.0 in 2023 webinar!

Supplier Cybersecurity Procurement Requirements – Survey
To support your cybersecurity action plans in meeting Rolls-Royce procurement requirements, please complete this survey to help us prioritize the information and resources you need.

Complete Your CMMC Assessment with Help from MxD
To help meet the necessary cybersecurity procurement requirements, RR is working with MxD to support suppliers in completing CMMC assessments and developing plan of action and milestones. We will walk you through what is needed and be available for any questions you may have. Get started here!

Action Required:

- If desired, sign up and attend the webinar on 22 March 2023.
- Complete the survey before the webinar.
- Visit the MxD cyber marketplace website to learn more.

Links:

Cyber Webinar Sign-Up Link: https://www.eventbrite.com/e/comply-with-cmmc-20-in-2023-tickets-525120869657

Survey Link:
https://forms.office.com/pages/responsepage.aspx?id=CrIkoBKIGkqwf_RRdL6YXiMbpbN_05JDk_bc3wBdTFpUMDFZTTlLODFTTUY4OThENTdCSlBSSk5DTi4u

Cyber Marketplace Link: https://www.mxdusa.org/marketplace/

NTS Category:

Regulatory/Legislation

Authorised by:

Jason Kasper
Procurement Development Executive