Toolkit for DoD Cyber Requirements

Guidance to suppliers for meeting Rolls-Royce standards

April 2025

Suppliers for Rolls-Royce's U.S. Department of Defense (DoD) product lines must meet the Rolls-Royce Supplier Minimum Cyber Security Standard. Suppliers must be compliant before receiving a new purchase order supporting a DoD contract.

Your company must:

- Comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which covers how to protect unclassified information in your system and includes performing a scored self-assessment.
- Submit your assessment score (less than three years old) to the DoD via the Supplier Performance Risk System (SPRS) website tool.
- Notify Rolls-Royce via our annual Procurement Information Booklet (PIB) — accessed through iValua — when the score is submitted.

Future DoD requirements:

Cybersecurity Maturity Model Certification (CMMC) 2.0 requirements will soon appear in DoD contracts. All Rolls-Royce suppliers that support DoD contracts must understand and abide by the CMMC Program.

US Defense requirements

Compliance with Defense Federal Acquisition Regulation Supplement (DFARS) requirements is a must to work on any DoD contract.

Key clauses already in effect are:

- DFARS 252.204-7012, which covers safeguarding of unclassified Covered Defense Information (CDI) and cyber incident reporting.
- This clause details how contractors must implement the 110 security controls stipulated in NIST SP 800-171 and when and how you must report cyber incidents to the DoD.
- DFARS 252.204-7019, which provides notice about assessment requirements including reporting scores to the DoD via SPRS.
- DFARS 252.204-7020, which expands on DFARS 7019, requiring contractors to ensure that subcontractors have submitted their assessment score to the DoD via SPRS.

Future key clauses are:

- DFARS 252.204-7021, which will require contractors to comply with the CMMC program and require contractors to flow down DFARS 252.204-7021 to subcontractors. DoD is updating 48 CFR Part 252.

Toolkit for DOD cyber requirements

Additional information

1. These requirements apply to all suppliers supporting DoD contracts. It applies to **FAR 12** and **FAR 15**. There are no geographic exceptions.
2. Registration in **SAM.gov** is required to submit your score into SPRS. Get help with SAM.gov here: **https://www.fsd.gov/gsafsd_sp**. Get SPRS help here: 207-438-1690 or **sprs-helpdesk@us.navy.mil**
3. Suppliers access the SPRS database through the **Procurement Integrated Enterprise Environment (PIEE)**. Get PIEE help here: 866-618-5988 or **disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil**
4. Cyber self-assessments should be started as soon as possible. You do not need access to SAM, PIEE, or SPRS to start your self-assessment.
5. Perfect scores are not required. NIST SP 800-171 allows a System Security Plan and Plan of Action and Milestones to address gaps.
6. SPRS assessment results cannot be more than three years old. If your assessment was performed more than three years ago, you must refresh it.
7. When suppliers submit their assessment results into SPRS, they log their results against their CAGE code. If a company has multiple CAGE codes, they must submit for all codes.
8. Rolls-Royce cannot view other companies' data via SPRS. Scores must be reported to us via the annual PIB to verify compliance.
9. For more information about the CMMC Program please see: **CMMC Program (DoD)** and **Rolls-Royce Supplier CMMC FAQ**.
10. Exceptions

- Commercial Off the Shelf (COTS) purchase orders. Something is considered COTS only if anyone can purchase it freely.
- Small orders up to the micro purchase threshold of $10,000.