Toolkit for MOD cyber requirements

Guidance to suppliers for meeting Rolls-Royce standards

Suppliers for Rolls-Royce's UK Ministry of Defence (MOD) product lines must meet the Rolls-Royce **Supplier Minimum Cyber Security Standard**. This Standard provides a flow-down of MOD cyber security requirements.

The **MOD Cyber Security Model** (CSM) ensures a risk-based proportionate approach is taken for protecting MOD information that is shared or created within the supply chain. Suppliers must be compliant with MOD cyber security requirements before receiving a purchase order or supporting a MOD contract. If not compliant with any cyber security requirements, suppliers must agree to a **Cyber Implementation Plan** (CIP) with their Rolls-Royce Buyer and include date(s) when they plan to become compliant.

Your company must:

- Comply with **Defence Condition 658** (DEFCON 658) and **Defence Standard 05-138** (DefStan 05-138), which cover how to protect MOD Identifiable Information (MODII) and organisational security and resilience.
- Complete the **Supplier Assurance Questionnaire** (SAQ) via the online MOD Supplier Cyber Protection Service. The SAQ determines compliance with DefStan 05-138.
- Understand that any non-compliant DefStan 05-138 requirements will be notified to your Buyer using a CIP.

Additionally, suppliers who receive/share OFFICIAL-SENSITIVE information must:

- Complete the Security Aspects Letter (SAL) response (**Annex A of ISN 2024/09**).
- Follow the F1686 Security Procedure (**ISN 2024/05**) and request approval from Rolls-Royce before subcontracting or sharing OFFICIAL-SENSITIVE information with sub-tier suppliers.

Compliance with DEFCON 658 requirements is a must to work on any MOD contract.

Key clauses are:

- 3.1.1, which covers safeguarding organisation systems and MOD data, compliance to DefStan 05-138 requirements, and preparation of the CIP.
- 3.1.2 and 3.1.3, which provide direction on the CSM, SAQ, and annual assessments.
- 3.1.5 and 3.1.6, which cover cyber security incident investigation and reporting. Suppliers should provide a prompt response and inform Rolls-Royce that mitigating action has been taken immediately. Report cyber security incidents to Rolls-Royce (see Section 1.7 of the **Supplier Minimum Cyber Security Standard** for information) and MOD Defence Industry Warning Advice and Reporting Point (WARP), in accordance with **ISN 2024/10**.

Additionally, contractors must ensure their subcontractors comply with DEFCON 658 and DefStan 05-138, as described in clause 3.1.1.

Toolkit for MOD cyber requirements

Additional information

1. These requirements apply to all suppliers supporting MOD contracts. There are no geographic exceptions.
2. Your buyer will inform you of the SAQ process. The SAQ is a self-assessment and completed annually.
3. When asked to do so, you should start the SAQ process without delay.
4. Perfect scores are not required. The SAQ process allows a CIP to address gaps.
5. **Cyber Essentials** certification is a baseline requirement for all MOD contracts. You should not wait for the SAQ process to start before obtaining your Cyber Essentials certificate.
6. Rolls-Royce cannot view other companies' data via SAQ. A new SAQ must be completed for each contract.
7. Suppliers shall keep and maintain, until six years after termination or end of contract term, all records to demonstrate compliance with DEFCON 658 and DefStan 05-138, and any information used to inform the risk assessment process (i.e., SAQ).
8. MOD may conduct audits to verify compliance to the DEFCON 658 and DefStan 05-138 requirements. They provide at least 15 days' calendar notice. In the event of a cyber security incident, audits by the MOD may be required to determine the cause and impact, and to verify the work conducted resolved the incident and mitigated the consequences.
9. Exceptions:

   Commercial Off the Shelf (COTS) purchase orders are exempt. Something is considered COTS only if anyone can purchase it freely.

Links for further information

- Guide to Defence Cyber Protection Partnership (DCPP) Cyber Security Model — including standards for version 3 and preparing for version 4: **Cyber Security Model - GOV.UK** containing links to:
  - DEFCON 658: **Defence Condition 658: cyber (flow-down) - GOV.UK**
  - DefStan 05-138 Issue 3: **Cyber security for defence suppliers (DefStan 05-138) - GOV.UK**
  - DefStan 05-138 Issue 4: **Cyber security for defence suppliers (DefStan 05-138, Issue 4) - GOV.UK**
  - Cyber Implementation Plan: **Cyber Implementation Plan (CIP) - GOV.UK**
  - **Supplier Assuranace Questionnaire (SAQ)**
- Industry Security Notice
  - ISN 2024/05 issued 15/04/2024 **Subcontracting or Collaborating on Classified UK MoD Programmes**
  - ISN 2024/09 Issued 19/08/2024 **Security Aspects Letters and Contractual Security Conditions**

SUPPLIER COMMUNICATION | Rolls-Royce's Global Supplier Portal is your first stop for information and documents, such as Notices to Suppliers (NTS). Go to suppliers.rolls-royce.com for more.