



Industry Security Notice

Number 2026/01 dated 30/03/2026

Subject: **Update to DEFSTAN 05-138 (Issue 4) covering narrative - Clarification to Cyber Security Model scope**

Introduction

1. This Industry Security Notice (ISN) has been prepared in support of supplier adoption of DEFSTAN 05-138 (Issue 4), published May 2024.
2. This ISN provides temporary replacement text for the covering text contained within that document, following update to the related DEFCON 658, ahead of any formal update to the document via DSTAN.

Applicability

3. This ISN applies to all suppliers engaged on contracts for which the UK MOD is a contracting party, or subcontracts thereof, to whom DEFSTAN 05-138 applies.

Issue

4. DEFSTAN 05-138 (Issue 4)¹, published May 2024, sets out controls applicable to the Cyber Security Model (CSMv4), compliance with which being further assured via certification to the corresponding level under the Defence Cyber Certification (DCC) scheme, which launched a year later in May 2025.
5. In addition to the controls set out within that standard, DEFSTAN 05-138 (Issue 4)

¹ https://assets.publishing.service.gov.uk/media/669923b249b9c0597fdaff90/Defence_Standard_05-138_Issue_4_-_cyber_security_for_defence_suppliers.pdf

contains overarching covering text that sets out the intended scope of application.

6. In response to industry request for further clarification of scope, the clarifying text attached at Annex A has been agreed, and published by means of this ISN in support of further uptake of that standard, in advance of any future update to that document via DSTAN.

Action by Industry

7. Suppliers are instructed to read the attached temporary replacement covering text for DEFSTAN 05-138 (Issue 4) in conjunction with existing contractual requirements.

Additional Information

8. It is expected that MOD project teams and SROs take additional notice of the implications of the enhanced organisational resilience requirements for supplier organisations as set out in DEFSTAN 05-138 (Issue 4) during its first year of operation [calendar year 2026], ensuring that such are taken into account when determining appropriate timescales for remediation.

9. If the content of this ISN conflicts with a contract-specific Security Aspects Letter (SAL), or for further information/clarification, please refer to your Delivery Team.

Validity / Expiry Date

10. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

11. The point of contact in respect of this ISN is:

Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
email: ukstratcomdd-cydr-csm@mod.gov.uk (Multiuser).

Annex A – Interim update to covering narrative – DEFSTAN 05-138 (Issue 4)

1 Introduction

1.1 The Ministry of Defence has adopted a risk-based, proportionate model and approach to strengthening resilience of its suppliers - the Cyber Security Model (CSM). A supplier that understands and protects its own critical business operations and continuity, in turn, protects its ability to support UK Defence.

1.2 The purpose of this Defence Standard is to define the required controls for each level of compliance within that model, aiding an organisation to protect its business-critical operations and maintain effective and proportionate cyber resilience.

1.3 The scope of this standard is intentionally broad. It ensures that a supplier organisation has the minimum level of controls required for its assigned Cyber Risk Profile (CRP) level, irrespective of any further controls required for a specific contracted output.

1.4 The requirements of this standard are:

- **‘Whole of organisation’ as applied to business-critical operations:** Requirements apply to a supplier’s approach to the cyber resilience of its business-critical operations across the supplier as a single legal entity.

For the purposes of this standard, business-critical operations are those activities, systems, assets and processes essential to the sustained operation of the supplier - where unavailability, inaccessibility or compromise would have a material adverse effect on the supplier’s ability to operate (which, in turn, protects its ability to support UK Defence).

As business-critical dependencies vary between suppliers, each organisation is responsible for determining and justifying these in the context of its own operational continuity requirements.

- **Applicable to any organisation:** The requirements set out within this standard can be applied by supplier organisations of any size or structure. Where specific controls may not reasonably apply due to the nature of an organisation’s operations, this should be discussed with the Defence Cyber Certification (DCC) certifying body, which can determine a proportionate interpretation without weakening the intent of the standard. Suppliers engaged, or who are looking to engage, under a UK Defence contract seeking to flag potential non-compliance are further advised to refer to Cyber Improvement Plan (CIP) process.

- **Proportionate / risk-based:** The minimum control requirements are determined by the CRP level assigned through the CSM. The assigned CRP level - not an organisation's internal cyber risk assessment – defines the minimum required controls.
- **Infrastructure-agnostic:** The controls within this standard apply to an organisation's business-critical operations, irrespective of a supplier's underlying infrastructure. Where business-critical operations rely on third-party services, suppliers must implement appropriate contractual, technical, and/or assurance measures to evidence that the controls within this standard are being met.

1.5 Validation of compliance with the requirements of this standard can be achieved and demonstrated through a supplier obtaining certification through the DCC scheme at the corresponding level (0-3). Certification of compliance applies only to the entity undergoing assessment - it does not automatically extend across wider corporate groups unless a group-level arrangement is explicitly justified and approved via the DCC certification authority.

1.6 Certification may be obtained irrespective of whether an organisation is currently engaged on a UK Defence contract. MOD may require certification as part of procurement; where suppliers are not yet certified, a contractual mechanism (CIP) exists to allow management of that situation under contract. It is anticipated that Level 0 certification will become a baseline requirement for Defence suppliers. Further guidance, including international considerations, on the application and interpretation of controls under DCC will be available via the certifying authority.

1.7 This Defence Standard does not replace any additional Defence or government requirements specific to system security, operational technology (OT), or the protection of classified data. Where such requirements exist, they will be defined separately, including but not limited to within government procurement notices, Defence Standards, DEFCONs or associated contractual documents (such as a Security Aspects Letter).

1.8 By applying this standard consistently across the Defence supply chain, MOD aims to raise the baseline organisational cyber resilience of its supply chain, reducing systemic risk and provide confidence that the defence supply chain can operate securely and resiliently in support of UK Defence.

2 Cyber Risk Profiles

2.1 The element of MOD's procurement process that concerns organisational cyber resilience within its supply chain is known as the Cyber Security Model (CSM). One output of applying the CSM during UK Defence procurement is the generation of a Cyber Risk Profile (CRP) level.

2.2 The CRP levels are:

- **Level 0 ('Basic')**
 - Assigned where there is a very low level of assessed cyber risk. It requires Supplier organisations to demonstrate basic cyber security practices.
- **Level 1 ('Foundational')**
 - Assigned where there is a low to moderate level of assessed cyber risk. It requires suppliers to demonstrate a comprehensive cyber security programme with good practices.
- **Level 2 ('Advanced')**
 - Assigned where there is a high level of assessed cyber risk. It requires suppliers to demonstrate advanced cyber security oversight and planning which drives robust organisational and cyber practices.
- **Level 3 ('Expert')**
 - Assigned where there is a substantial level of assessed cyber risk to a Supplier. It requires suppliers to demonstrate expert cyber security capabilities that apply a 'defence in depth' methodology to appropriately protect the organisation against new and evolving threats.

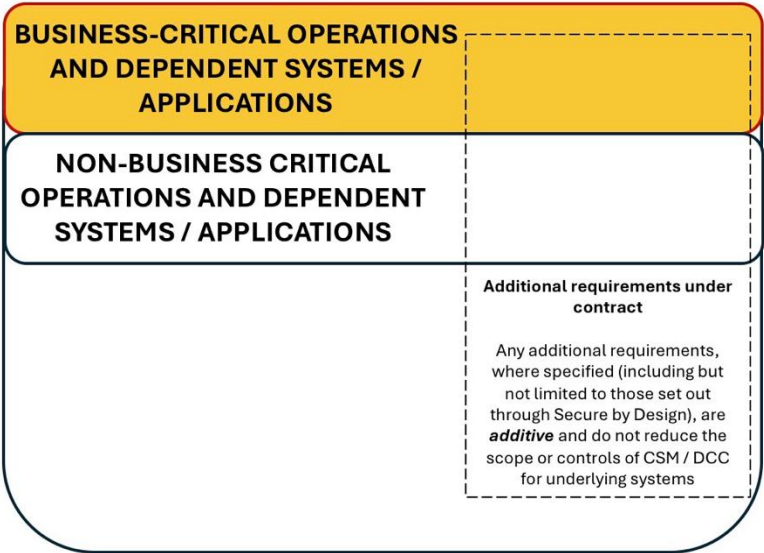
2.3 Where a supplier delivers multiple contracts with different CRP levels, the supplier shall maintain certification at the highest applicable level. Certification at a higher level is deemed to satisfy all lower-level requirements.

2.4 The control requirements for each level are set out in Clause 3.

2.5 The supplier shall ensure that each control requirement in Clause 3 is supported by a documented and implemented control, with auditable evidence available. Maintaining this documentation is also a requirement for ongoing DCC certification.

2.6 Where the term 'Functions' is used in Clause 3, suppliers should have regard to the guidance relating to business-critical activities set out in section 1 of this document.

2.7 Where the term 'Data' is used in Clause 3, suppliers should consider such as being: any data or information, irrespective of ownership that is generated, handled, stored or otherwise processed by the supplier as necessary to carry out their Functions.



KEY:

