CYBER SECURITY MODEL (VERSION 4) - CYBER IMPROVEMENT PLAN

The following document is to be used in instances where a supplier Self Assessment Questionnaire (SAQ) provided under the Cyber Security Model (CSM) is submitted as 'non-compliant' with the requirement set out as associated with an associated Risk Assessment Reference (RAR).

Supplier Organisation Name:	[To be completed]
Supplier Contact Name:	[To be completed]
Supplier Contact Email:	[To be completed]
Contract Name / Reference:	[To be completed]
Risk Assessment Reference (RAR):	[To be completed]
Supplier Assurance Questionnaire (SAQ) reference:	[To be completed]

REQUIREMENT

Control level requirement – as stated on the ITT	
Required Level:	**Level [0 / 1 / 2 / 3]**
Required assurance level:	**[Self-attested / Certified]**

COMPLETED BY SUPPLIER

Response (please delete as necessary)	
Current level:	**NONE or Level [0 / 1 / 2 / 3]**
Current assurance level:	**[Self-attested / Certified]**
	If Certified, please provide certificate reference: **[INSERT REFERENCE]**

Proposed level of compliance:	**Delivery by:**	**Level of assurance:**	**Comments:**
Level [0 / 1 / 2 / 3]	[Contract award / Date (DD-MMMM-YYYY)]	[Self-attested / Certified]	[To be completed]

The completed Cyber Improvement Plan (CIP) must be returned to the relevant MoD Contracting / Delivery Team for the contract / procurement in question.

Note: Upon agreement of a CIP, the relevant MOD Contracting / Delivery Team will ensure that the activity is further encapsulated by the addition of relevant elements under a milestone payment condition and tracked as a contract deliverable via a schedule to the contract.

Should the contracting parties agree that additional information in support of a CIP is necessary to enable the effective monitoring / support of such an arrangement, such must be documented.

(Optional) Additional supporting notes: