SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

DCPP

Becoming MOD cyber-ready
WHY IS IT HAPPENING
Cyber security risks are real and UK MOD is taking appropriate steps to protect their data and ensure it is handled with the appropriate level of care. This means that everyone in the supply chain, from the largest prime to the smallest component manufacturer, must prove that they can be trusted to handle the MOD’s data and not put the security of the defence industry at risk.

WHAT DO SUPPLIERS NEED TO DO?
Suppliers may be asked to complete a Supplier Assurance Questionnaire (SAQ) and provide suitable supporting evidence to demonstrate ability to meet the DCPP requirements for the level of risk that they are, or will be, contracted against.

WHAT'S CHANGED?
DEFCON 658 stipulates that all suppliers bidding on new MOD contracts which necessitate transfer of ‘MOD identifiable information’, need to implement and demonstrate compliance against a range of controls as determined through a Risk Assessment process defined in DEFSTAN05-138.

WHAT ARE THESE REQUIREMENTS?
Each requirement is made up of a series of individual controls that suppliers need to implement to demonstrate compliance. The number of requirements for each risk profile is outlined in the diagram below. Requirements are progressive as you move up the risk profiles, so the lower levels are the foundation of the higher levels and each level builds on the ones before.

WHY MUST I COMPLY?
➢ Failure to comply will exclude Suppliers from all new, or renewing, contracts post April 2017
➢ It’s a Supplier’s choice to remain compliant. Contracts can be won or lost without having the necessary evidence in place to support their Cyber Security Maturity

THALES HERE TO HELP
Thales has already been exposed to the DCPP CSM Requirements as part of the working group to support the construct of the overarching Governance, including the formulation of the Requirements themselves.
Thales continues to collaborate with the DCPP as part of the continual improvement ethos.
Thales is committed in promoting the importance of adopting a good cyber security culture/posture throughout the Supply Chain, allowing them to become better equipped to protect their businesses against the Cyber Threat.

N/A
No action required

Very Low
1 very low control
Cyber Essentials

Low
16 low controls
including Cyber Essentials Plus

Moderate
16 low controls
including Cyber Essentials Plus
+16 low control
including Cyber Essentials Plus
+16 moderate controls
+12 high controls