DCPP Overview

Defence Cyber Protection Partnership

The Defence Cyber Proptection Partnership (DCPP) is a joint UK Ministry of Defence (MOD) and industry initiative put in place to improve the protection of the defence supply chain against cyber threats. Applicable contracts will undergo a risk assessment to determine a cyber risk profile and the requirements on the supplier. Suppliers demonstrate compliance with these requirements via the online Supplier Cyber Protection Service.

Cyber Security Model

The Cyber Security Model (CSM) developed by the DCPP and being rolled out by the MOD is intended to ensure that **MOD Identifiable Information** is adequately protected. The CSM consists of the following three elements:

1. The risk assessment process; used to measure the level of cyber risk for a contract;
2. The requirements that a supplier will be required to achieve for the level of assessed cyber risk is determined by the risk assessment. These requirements are detailed in Def Stan 05-138: Cyber Security for Defence Suppliers; and
3. The supplier assurance questionnaire (SAQ) via the Supplier Cyber Protection Service; the means by which a supplier demonstrates their compliance with the cyber requirements.

If a contract contains MOD Identifiable Information then the Cyber Security Model is applicable through DEFCON 658 and DEF STAN 05-138. This must be flowed down through the supply chain until no MOD Identifiable Information is contained or generated within a contract.

Cyber Essentials Scheme

The Cyber Essentials Scheme defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats coming from the Internet. In particular, it focuses on threats

which require low levels of attacker skill, and which are widely available online.

The Cyber Essentials Scheme is the basis upon which DCPP is built. As of 1 January 2016, all suppliers with MOD contracts that contain MOD Identifiable Information are required to have the Cyber Essentials Scheme (CES) Certification.

Cyber Essentials Plus provides an independent penetration test and site assessment of your Cyber Essentials responses.

Risk Profiles Summary

The cyber risk profile of a contract – 'Not Applicable' (N/A), 'Very Low' (VL), 'Low' (L), 'Moderate' (M) or 'High' (H) – determines the number of applicable requirements. Requirements are grouped into risk areas. 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 below.

UK - DCPP	N/A	VL	L	M	H
Technology		1*	5	7	10
Governance			2	1	
Culture & Awareness			3	2	
Personnel			3	3	
Risk Management				1	
Info Management			2	3	
Incident Management			1		1
Total Requirements	**0**	**1***	**17**	**33**	**44**

*This Requirement, Cyber Essentials Scheme, comprises 26 controls.

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. Accreditation with the Cyber Essentials Scheme is the minimum requirement for contracts that contain MOD Identifiable Information and is the only requirement for a Very Low risk profile. Cyber Essentials Plus is required for a Low, Moderate and High risk profile. Suppliers must be fully compliant with all the requirements for the assessed risk profile; full details of Def Stan 05-138 requirements can be found detailed in the DCPP Cyber Risk Profile Control Guidance.

While suppliers need only comply with the requirements for the assessed risk profile it would be beneficial, to them, to implement requirements from higher risk profiles so as to better improve their protection from cyber threat.

All companies are encouraged to attain accreditation with the Cyber Essentials scheme as part of best practice, regardless of whether they hold contracts that contain or generate MOD Identifiable Information.

Defcon and Def Stan Overview

The DCPP is governed by two documents; the Defence Condition, Defcon 658, which is flowed down in contracts and the Defence Standard, Def Stan 05-138, which can defines the overall process and requirements.

Defcon	Def Stan
Authority Obligations: Define Risk Level and Notify of any changes Contractor Obligations: Compliance to Risk Profile Requirements, Ensure appropriate flow-down to suppliers and Report Cyber Incidents and Investigate potential incident Retain Records for 6-years post contract close Authority has the Rights to Audit Defines Termination Rights	When and How to conduct a Risk Assessment How to demonstrate compliance through the CSM Digital Service Definition of each Cyber Risk Profile How to deal with Non-Compliance and the Risk Acceptance Process: Cyber Implementation Plans and Unmitigated Risk Acceptance process Visibility of Data Validity of Response International and Other Equivalence

Useful Areas for Additional Information

Check out www.gov.uk/mod/dcpp

Achieve Cyber Essentials

www.cyberstreetwise.com/cyberessentials/

Ask your information security staff to join Cyber Security Information Sharing Partnership (CiSP) to access threat information

http://www.cisp.org.uk/