Ministry of Defence

Defence Standard 05-138

Issue 3 **Date:** **28 June 2021**

Cyber Security for Defence Suppliers

Section 1

Foreword

Defence Standard Structure

Section 1 Revision Note

- Historical Record
- Warning
- Standard Clauses

Section 2

- Title
- Introduction
- Table of Contents
- Scope
- Technical Information to include Tables and Figures
- Annexes

Section 3

- Normative References
- Definitions
- Abbreviations

REVISION NOTE

This update concentrates on an updated set of cyber security controls. Most of the Cyber Security Model process has been taken out as this document focuses on the relationship between the Cyber Risk Profile and the security controls.

HISTORICAL RECORD

This standard supersedes the following:

Defence Standard 05-138 Issue 2

WARNING

The Ministry of Defence (MOD), like its contractors, is subject both to United Kingdom law and any EU-derived law that has been retained under the European Union (Withdrawal) Act 2018 regarding Health and Safety at Work. Many Defence Standards set out processes and procedures that could be injurious to health if adequate precautions are not taken. Adherence to those processes and procedures in no way absolves users from complying with legal requirements relating to Health and Safety at Work.

STANDARD CLAUSES

a) This standard has been published on behalf of the Ministry of Defence (MOD) by UK Defence Standardization (DStan).

b) This standard has been reached following broad consensus amongst the authorities concerned with its use and is intended to be used whenever relevant in all future designs, contracts, orders etc. and whenever practicable by amendment to those already in existence. If any difficulty arises which prevents application of the Defence Standard, DStan shall be informed so that a remedy may be sought.

c) Please address any enquiries regarding the use of this standard in relation to an invitation to tender or to a contract in which it is incorporated, to the responsible technical or supervising authority named in the invitation to tender or contract.

d) Compliance with this Defence Standard shall not in itself relieve any person from any legal obligations imposed upon them.

e) This standard has been devised solely for the use of the MOD and its contractors in the execution of contracts for the MOD. To the extent permitted by law, the MOD hereby excludes all liability whatsoever and howsoever arising (including, but without limitation, liability resulting from negligence) for any loss or damage however caused when the standard is used for any other purpose.

Section 2

Cyber Security for Defence Suppliers

0 Introduction

a) The Defence Cyber Protection Partnership (DCPP) is a joint Ministry of Defence (MOD) / Industry initiative formed as part of the Defence Suppliers' Forum's directive to improve the protection of the defence supply chain from the cyber threat.

b) The DCPP acts in support of the UK's National Security Strategy and the National Cyber Security Strategy, which reaffirm the cyber threat as a Tier One risk to UK interests.

c) The Cyber Security Model is a risk-based proportionate approach to protecting MOD information as it moves through, or is generated in, the supply chain.

Contents

0 Introduction 2-1

1 Scope 2-3

2 Reporting of Incidents 2-3

Annexes

Annex A Cyber Risk Profiles 2-4

Annex B MOD Identifiable Information 2-11

Tables

Table A.1 – DCPP Cyber Risk Profile – Very Low 2-5

Table A.2 – DCPP Cyber Risk Profile – Low 2-6

Table A.3 – DCPP Cyber Risk Profile – Moderate 2-7

Table A.4 – DCPP Cyber Risk Profile – High 2-9

Table B.1 – Illustrative Criteria 2-12

1 Scope

1.1 This Defence Standard defines the MOD requirements in respect of the Cyber Security Model (CSM). The CSM starts with a Risk Assessment. This generates a Cyber Risk Profile, as broadly explained in Annex A. Each Cyber Risk Profile has security requirements, also identified in Annex A.

2 Reporting of Incidents

2.1 Any cyber security incident known or believed to involve MOD Identifiable Information (MODII) must notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Contractors NSA/DSA , and in the case of a Sub-contractor also notify the Contractor, immediately in writing as soon as they know or believe that a Cyber Security Incident has or may have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available.

Annex A

Cyber Risk Profiles

A.1 Cyber Risk Profiles

a) There are five outcomes from the Risk Assessment process. These Cyber Risk Profiles are: Not Applicable, Very Low, Low, Moderate and High.

b) Every MOD requirement must be subject to a Risk Assessment and have one of these five profiles assigned. The CRP are related to appropriate controls detailed in this document.

c) Contracts which do not involve MODII will be deemed to carry no cyber risk and assessed as 'Not Applicable'.

d) There is no specific correlation between the Risk Assessment outcome and the Government Security Classification Scheme although contracts involving Secret and Top Secret information would be expected to carry a moderate or high level of cyber risk.

e) An explanation of the Cyber Risk Profiles is below:

1) **Not Applicable**
The Not Applicable outcome does not require specific cyber control measures although it is recommended that all suppliers, as a matter of good practice, achieve compliance with the Cyber Essentials Scheme as a minimum where they use IT systems for conducting business.

2) **Very Low**
The Very Low CRP applies to contracts where it has been assessed the cyber risks to the MOD from the contract will be deemed basic and untargeted. The control measures required to mitigate the cyber risks are shown in Annex A Table A.1.

3) **Low**
The Low CRP applies to contracts where it has been assessed the cyber risks to the contract may be basic but are more targeted and where the attackers may be semi-skilled but not persistent. The control measures required to mitigate the cyber risks are shown in Annex A Table A.2.

4) **Moderate**
The Moderate CRP applies to contracts where it has been assessed the cyber risks to the contract are more advanced. Cyber-attacks may be tailored and targeted with an objective of gaining access to a specific asset(s) or to enable a denial of service. The control measures required to mitigate the cyber risks are shown in Annex A Table A.3.

5) **High**
The High CRP applies to contracts where it has been assessed the cyber risks to the contract may be subjected to Advanced Persistent Threats (APT). Attackers at this level will typically be organised, highly sophisticated, well-resourced and persistent. APT attacks may be sustained over long periods and the attack may lay dormant for months or years after an initial approach. The control measures required to mitigate the cyber risks are shown in Annex A Table A.4.

Table A.1 – DCPP Cyber Risk Profile – Very Low

Very Low CRP Requirements
Info-Cyber Systems Security
VL.01 Maintain annually renewed Cyber Essentials Scheme certification.

Table A.2 – DCPP Cyber Risk Profile – Low

Low CRP Requirements
Governance
L.01 Define and implement an information security policy, related processes and procedures.
L.02 Define and assign information security relevant roles and responsibilities.
L.03 Define and implement a policy which addresses information security risks within the supply chain.
Security Culture and Awareness
L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.
L.05 Define employee (including contractor) responsibilities for information security.
L.06 Define and implement a policy to provide employees and contractors with information security training.
Information Asset Security
L.07 Define and implement a policy for ensuring sensitive information is clearly identified.
L.08 Define and implement a policy to control access to information and information processing facilities.
Info-Cyber Systems Security
L.09 Maintain annually renewed Cyber Essentials Scheme Plus Certification.
L.10 Define and implement a policy to control the exchanging of information via removable media.
L.11 Record and maintain the scope and configuration of the information technology estate.
L.12 Define and implement a policy to manage the access rights of user accounts.
L.13 Define and implement a policy to maintain the confidentiality of passwords.
Personnel Security
L.14 Define and implement a policy for verifying an individual's credentials prior to employment.
L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.
Security Incident Management
L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.

Table A.3 – DCPP Cyber Risk Profile – Moderate

Moderate CRP Requirements	
Security Governance	
L.01 Define and implement an information security policy, related processes and procedures.	
L.02 Define and assign information security relevant roles and responsibilities.	
L.03 Define and implement a policy which addresses information security risks within supplier relationships.	
M.01 Define and implement a policy which provides for regular, formal information security related reporting.	
M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.	
Security Culture and Awareness	
L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.	
L.05 Define employee (including contractor) responsibilities for information security.	**M.03** Define and implement a repeatable risk assessment process.
L.06 Define and implement a policy to provide employees and contractors with information security training.	
Information Asset Security	
L.07 Define and implement a policy for ensuring sensitive information is clearly identified.	**M.04** Define and implement a policy for storing, accessing, and handling sensitive information securely.
M.05 Define and implement a policy for data loss prevention**.**	
M.06 Define, implement and test a policy for regular off-line back-up of data off-site.	
L.08 Define and implement a policy to control access to information and information processing facilities.	**M.07** Ensure the organisation has identified asset owners and asset owners control access to their assets.
Info-Cyber Systems Security	
L.09 Maintain annually renewed Cyber Essentials Scheme Plus Certification.	
L.10 Define and implement a policy to control the exchanging of information via removable media.	
L.11 Record and maintain the scope and configuration of the information technology estate.	
M.08 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.	
M.09 Undertake administration access over secure protocols, using multi-factor authentication.	
M.10 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	

Moderate CRP Requirements	
L.12 Define and implement a policy to manage the access rights of user accounts.	**M.11** Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.12 Define and implement a policy to control remote access to networks and systems.	
L.13 Define and implement a policy to maintain the confidentiality of passwords.	
M.13 Define and implement a policy to control the use of authorised software.	
M.14 Define and implement a policy to control the flow of information through network borders.	
Personnel Security	
L.14 Define and implement a policy for verifying an individual's credentials prior to employment.	**M.15** Define and implement a policy for applying security vetting checks to employees.
L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.	
M.16 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.	
M.17 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	
Security Incident Management	
L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.	

Table A.4 – DCPP Cyber Risk Profile – High

High CRP Requirements	
Security Governance	
L.01 Define and implement an information security policy, related processes and procedures.	
L.02 Define and assign information security relevant roles and responsibilities.	
L.03 Define and implement a policy which addresses information security risks within supplier relationships.	
M.01 Define and implement a policy which provides for regular, formal information security related reporting.	
M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.	
Security Culture and Awareness	
L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.	
L.05 Define employee (including contractor) responsibilities for information security.	**M.03** Define and implement a repeatable risk assessment process.
L.06 Define and implement a policy to provide employees and contractors with information security training.	
Information Asset Security	
L.07 Define and implement a policy for ensuring sensitive information is clearly identified.	**M.04** Define and implement a policy for storing, accessing, and handling sensitive information securely.
M.05 Define and implement a policy for data loss prevention	
M.06 Define, implement and test a policy for regular off-line back-up of data off-site.	
L.08 Define and implement a policy to control access to information and information processing facilities.	**M.07** Ensure the organisation has identified asset owners and asset owners control access to their assets.
Info-Cyber Systems Security	
L.09 Maintain annually renewed Cyber Essentials Scheme Plus Certification.	
H.01 Maintain patching metrics and assess patching performance against policy.	
H.02 Ensure wireless connections are authenticated.	
L.10 Define and implement a policy to control the exchanging of information via removable media.	
L.11 Record and maintain the scope and configuration of the information technology estate.	
M.08 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.	
M.09 Undertake administration access over secure protocols, using multi-factor authentication.	

High CRP Requirements	
M.10 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	**H.03** Deploy network monitoring techniques which complement traditional signature-based detection.
	H.04 Place application firewalls in front of critical servers to verify and validate the traffic going to the server.
	H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.
L.12 Define and implement a policy to manage the access rights of user accounts.	**M.11** Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.12 Define and implement a policy to control remote access to networks and systems.	
L.13 Define and implement a policy to maintain the confidentiality of passwords.	
M.13 Define and implement a policy to control the use of authorised software.	**H.06** Define and implement a policy to control installations of and changes to software on any systems on the network.
M.14 Define and implement a policy to control the flow of information through network borders.	**H.07** Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.
H.08 Design networks incorporating security countermeasures, such as segmentation or zoning.	
H.09 Ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.	
Personnel Security	
L.14 Define and implement a policy for verifying an individual's credentials prior to employment.	**M.15** Define and implement a policy for applying security vetting checks to employees.
L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.	
M.16 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.	
M.17 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	
Security Incident Management	
L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.	
H.10 Proactively verify security controls are providing the intended level of security.	
H.11 Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis	

Annex B

MOD Identifiable Information

B.1 The definition of MOD Identifiable Information (MOD II) is as follows:

All Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure.

Note 1. "Electronic Information" is defined in DEFCON 658.

B.2 The definition of MOD II is intentionally broad, as it is envisaged that most MOD acquisitions will involve MOD II. There will be some exceptions, therefore it is essential to consider each requirement on a case-by-case basis and adopt a reasonable, pragmatic and proportionate approach when deciding what you should class as within scope.

B.3 The fact that MOD is the customer does not automatically make information 'MOD II'. Information will not be considered to be MOD II where it is already in the public domain (otherwise than by a breach of any contractual or common law duty of confidentiality).For example, COTS Product Information would not be considered MOD II, therefore unless other information suggests sensitivity (see next clause), it is likely that a COTS acquisition would not fall within the scope of MOD II.

B.4 The list of illustrative criteria in Annex B Table B.1 below is a guide of the factors to consider when deciding if a requirement is within the scope of MOD II. It is not a definitive list and it is important to consider the acquisition as a whole when considering whether it will involve MOD II. For example, procurement of a particular widget may not be identifiable with a defence capability if viewed in isolation, however other details (such as the specific quantity and classified delivery address) could reveal information which could be useful to a potential adversary.

B.5 Information will not be considered to be MOD II where it is already in the public domain otherwise than by a breach of any contractual or common law duty of confidentiality.

Table B.1 – Illustrative Criteria

Illustrative Criteria Information which would **typically be excluded** from MOD Identifiable Information (unless notified otherwise in writing)	Information which would **typically be included** in MOD Identifiable Information (unless notified otherwise in writing)
Contract Name (unless specified in a contract specific Security Aspects Letter (SAL)) Contract Number (unless specified in a contract specific SAL) Quantity and Delivery schedule (unless specified in a contract specific SAL) Delivery Address (unless specified in a contract specific SAL) DEFCONs and Def Stans Standard contract Text AQAP Quality Conditions Standard Industry / Commercial accreditation (e.g. BS Standards) Company Proprietary Information COTS (Commercial Off The Shelf) product information	MOD Statements of Work (SOW) MOD Technical Requirements MOD Acceptance and Test Parameters (and corresponding results) MOD Drawings and documents MOD Interface Drawings / Documents Documents marked as OFFICIAL SENSITIVE or with any form of handling instruction Anything covered by a SAL (which always take precedence) Foreground Intellectual Property Personal Data / Medical records and all information covered by the Data Protection Act (DPA) Firmware / Software deliverables MOD Marked Property and Equipment, including “free issue” and temporary loan assets (Government Furnished Equipment (GFE)) Contract Data Requirements List (CDRL) i.e. data deliverables Industry provide to the MOD under the contract and which effectively become MOD property.

Section 3

Normative References

1 The publications shown below are referred to in the text of this standard. Publications are grouped and listed in alpha-numeric order.

Note: Def Stan's can be downloaded free of charge from the DStan web site by visiting **<http://dstan.uwh.diif.r.mil.uk/>** for those with RLI access or **<https://www.dstan.mod.uk>** for all other users. All referenced standards were correct at the time of publication of this standard (see 2, 3 & 4 below for further guidance), if you are having difficulty obtaining any referenced standard please contact the DStan Helpdesk in the first instance.

Def Stans

Number	Title

STANAGs

Number	Title

Allied Publications

Number	Title

Other References

Standard Type	Standard Name
Other Civilian/Industry Standards	ISN 2017/03 - REQUIREMENT TO REPORT SECURITY INCIDENTS AFFECTING MOD MATERIAL TO THE MOD

2 Reference in this Standard to any normative references means in any Invitation to Tender or contract the edition and all amendments current at the date of such tender or contract unless a specific edition is indicated. Care should be taken when referring out to specific portions of other standards to ensure that they remain easily identifiable where subsequent amendments and supersession's might be made. For some standards the most recent editions shall always apply due to safety and regulatory requirements.

3 In consideration of clause 2 above, users shall be fully aware of the issue, amendment status and application of all normative references, particularly when forming part of an Invitation to Tender or contract. Correct identification of standards is as defined in the ITT or contract.

4 DStan can advise regarding where to obtain normative referenced documents. Requests for such information can be made to the DStan Helpdesk. Details of how to contact the helpdesk are shown on the outside rear cover of Defence Standards.

Definitions

For the purpose of this standard, ISO/IEC Guide 2 ‘Standardization and Related Activities – General Vocabulary’ and the definitions shown below apply.

Definition	Description
The Authority	The Authority is the role which determines the Cyber Risk Profile appropriate to a contract and, where the supplier has not already been notified of the Cyber Risk Profile prior to the date of a contract, shall provide notification of the relevant Cyber Risk Profile to the supplier as soon as is reasonably practicable; and notify the supplier as soon as reasonably practicable where The Authority reassesses the Cyber Risk Profile relating to that Contract (from DEFCON 658 which remains the authority on defining The Authority).
Accreditation	Accreditation means accredited by the MOD or by an authority whose accreditation is acceptable to the MOD.
Defence	The term Defence relates to all parts of the MOD which includes the Royal Navy, the British Army, the Royal Air Force, all Trading Funds, all Non Departmental Public Bodies and MOD Head Office.
Defence Supply Chain	All companies and organisations which are contracted to provide goods or services to Defence whether through a contract directly awarded by MOD or through a contract sublet by a MOD supplier.
Cyber Risk	In its broadest form, cyber risk is synonymous with IT risk – that is, “the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise” (ISACA IT Risk Framework). Further detail on Cyber Risk is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf .
Cyber Risk Profile	A Cyber Risk Profile is the outcome of a Risk Assessment, which defines a set of proportionate mitigation requirements based on the level of assessed cyber risk (impact x likelihood) to a MOD contract.
Cybersecurity	ISACA’s definition of cyber security is: “The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.”
MOD Accreditor	An Accreditor is the individual responsible for providing the Risk Owner with a formal, independent assessment of an information or cyber system against its security requirements, balancing any residual risks in the context of the business requirement. To request an Accreditor see: https://www.gov.uk/government/publications/industry-accreditation-request-form

MOD Identifiable Information	As defined in DEFCON 658, Industry Security Notice 2017/04 (subject to update) and at Annex C. DEFCON 658 remains the authority on defining MODII.
Risk	Risk is 'a future uncertain event that could influence the achievement of objectives and statutory obligations.' Risk is assessed in terms of likelihood and impact using both qualitative and quantitative methods, and judgement borne of an individual or group(s) of Subject Matter Experts. In summary, Risk = Impact (Value x Criticality) x Likelihood (Threat x Vulnerability). (JSP 440 Part 2 v6.0).
Supplier Cyber Protection	Supplier Cyber Protection (previously known as Octavian) is the online tool developed in partnership with industry and delivered by a third-party, which is utilised for the completion of Risk Assessments and Supplier Assurance Questionnaires. Certain users have enhanced access and are able to interrogate the data for business improvement and risk management purposes.

Abbreviations

Abbreviation	Description
APT	Advanced Persistent Threats
AQAP	Allied Quality Assurance Publication
BS	British Standard
CDRL	Contract Data Requirements List
CES	Cyber Essentials Scheme
CES+	Cyber Essentials Scheme Plus
CIP	Cyber Implementation Plan
COTS	Commercial Off The Shelf
CRP	Cyber Risk Profile
CSM	Cyber Security Model
DCPP	Defence Cyber Protection Partnership
DEFCON	Defence Condition
Def Stan	Defence Standard
DPA	Data Protection Act
DSA	Designated Security Authority
DStan	UK Defence Standardization
GFE	Government Furnished Equipment
IDS	Intrusion Detection System
ISACA	Information Systems Audit and Control Association
ISN	Industry Security Notice
IT	Information Technology
ITT	Invitation To Tender
JSP	Joint Service Publication
JSyCC	Joint Security Co-ordination Centre
MOD	Ministry of Defence

MODII	MOD Identifiable Information
NSA	National Security Authority
RA	Risk Assessment
RAR	Risk Assessment Reference
RLI	Restricted LAN Interconnect
SAL	Security Aspects Letter
SAQ	Supplier Assurance Questionnaire
SIRO	Senior Information Risk Owner
SOW	Statement Of Work
UK	United Kingdom
WARP	Warning, Advice and Reporting Point

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

UK Defence Standardization Help Centre

Please direct any enquiries via the Standardization Management Information System (StanMIS) Help Centre.

To access the StanMIS Help Centre please select either http://stanmis.gateway.isg-r.r.mil.uk/ (for MOD and industry users with MOD Core Network (MCN) access) or https://www.dstan.mod.uk/StanMIS/ (for all other users), and, after logging in, please follow the link to the Help Centre. If required, users can also register for an account from the login screen.

File Reference

The DStan file reference relating to work on this standard is 01142/2019.

Contract Requirements

When Defence Standards are incorporated into contracts, users are responsible for their correct application and for complying with contractual and statutory requirements. Compliance with a Defence Standard does not in itself confer immunity from legal obligations.

Revision of Defence Standards

Defence Standards are revised as necessary by an up-issue or amendment. It is important that users of Defence Standards ensure that they are in possession of the latest issue or amendment. Information on all Defence Standards can be found on the DStan Websites https://www.dstan.mod.uk and http://dstan.uwh.diif.r.mil.uk/, updated weekly. Any person who, when making use of a Defence Standard, encounters an inaccuracy or ambiguity is encouraged to notify UK Defence Standardization (DStan) without delay in order that the matter may be investigated and appropriate action taken.