Ministry of Defence

Defence Standard 05-138

Issue 2 **Date: 28 September 2017**

Cyber Security for Defence Suppliers

Section 1

Foreword

Defence Standard Structure

Section 1 (Generated by the StanMIS toolset)

- Revision Note
- Historical Record
- Warning
- Standard Clauses

Section 2 (Technical information provided by Subject Matter Expert)

- Title
- Introduction (optional)
- Table of Contents
- Scope
- Technical Information to include Tables and Figures
- Annexes (as required)

Section 3 (Generated by StanMIS toolset)

- Normative References
- Definitions
- Abbreviation

REVISION NOTE

The key changes are:

Simplification of the wording of H10 which refers to Data Loss Prevention and an additional control added at High.

Improvements in the text to outline the Cyber Security Model including the adoption of common terminology throughout the document.

Inclusion of the definition of MOD Identifiable Information (MODII)

Textual changes to align with JSP440 terminology to deliver common language across Defence and its partners.

DETAIL

The text has been updated and now refers to five Cyber Risk Profiles, which are the outcomes of a Risk Assessment. The Cyber Security Model is explained twice, once in outline at the start of the document and a second time in more detail later. Further detail has been added to explain how a Cyber Implementation Plan is considered.

The definition of MODII has been added so there is no requirement to source the definition from DEFCON658, although DEFCON658 remains the authoritative document.

Changes to technical controls:

1. DEFSTAN 05-138 v1:

H.10 Ensure Data Loss Prevention (DLP) at network egress points to inspect the contents of and, where necessary, block information being transmitted outside of the network boundary.

v2 of DEFSTAN 05-138:

H.10 Ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.

2. v2: H.12 Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis

3. Headings

4. DEFSTAN 05-138 v1:	v2 of DEFSTAN 05-138:
Technology and Services	Info-Cyber Systems Security

5. DEFSTAN 05-138 v1:	v2 of DEFSTAN 05-138:
Good Governance	Security Governance

6. DEFSTAN 05-138 v1:	v2 of DESTAN 05-138:
Culture and Awareness	Security Culture and Awareness
7. DEFSTAN 05-138 v1:	v2 of DEFSTAN 05-138:
Information	Information Asset Security
8. DEFSTAN 05-138 v1:	v2 of DEFSTAN 05-138:
Preparing for and responding to Security Incidents	Security Incident Management

HISTORICAL RECORD

This standard supersedes the following:

Def Stan 05-138 Issue 1

WARNING

The Ministry of Defence (MOD), like its contractors, is subject to both United Kingdom and European laws 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

0.1 The Defence Cyber Protection Partnership (DCPP) is a joint Ministry of Defence (MOD) / Industry initiative initiated in 2012 and formally established in 2013 as part of the Defence Suppliers' Forum's directive to improve the protection of the defence supply chain from the cyber threat. The partnership consists of: the MOD, defence primes, two trade associations (ADS and techUK), the Department for Digital, Culture, Media & Sport and the National Cyber Security Centre.

0.2 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.

Contents

1. A Key Output of the DCPP

1.1 One of the key outputs was to develop a set of proportionate cyber security standards which could be included in all MOD contracts. This objective has been achieved by the implementation of the Cyber Security Model (CSM).

2. The Cyber Security Model in Outline

2.1 The Cyber Security Model (CSM) consists of 3 elements and is conducted using an online tool, Octavian. The three main components of the CSM are detailed below:

a. First, a Risk Assessment (RA) is conducted to evaluate the degree of cyber risk to a specific contract and establish a Cyber Risk Profile;

b. Second, a Supplier Assurance Questionnaire (SAQ), is completed by suppliers who wish to be considered for a contract;

c. Third, an evaluation of the SAQ and any supporting evidence, such as a Cyber Implementation Plan (CIP), by The Authority which will form a factor in considering if a contract should be awarded.

2.2 This Defence Standard sets out the details of the CSM, the supporting information required to use it and the controls a supplier will be required to achieve for each level of assessed cyber risk.

3. Applicability

3.1 This standard shall be used by all involved in awarding contracts on behalf of the MOD including where suppliers subcontract elements of their contract to other suppliers, regardless of the nationality or location of the supplier.

3.2 This standard specifies the measures Defence Suppliers are required to achieve at each of the levels of cyber risk a contract can be assessed as carrying. This standard is applicable to all MOD procurements, MOD Suppliers and their subcontract suppliers which have a relationship to one or more MOD contracts.

4. Warning

4.1 The MOD, like its contractors, is subject to both United Kingdom and European laws regarding Health and Safety at Work. Many Defence Standards set out processes and procedures which 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.

5. The Cyber Security Model in Detail

5.1 Risk Assessment

a. As part of the procurement process in the MOD The Authority[1] must complete a Risk Assessment (RA) for all requirements.

b. A RA is completed by logging onto Octavian and completing a risk assessment questionnaire. The output of a RA is one of five Cyber Risk Profiles, which are: Not Applicable, Very Low, Low, Moderate and High. On completion, each RA will receive a risk assessment reference (RAR) number. Any contract which involves the transfer or creation of MODII as part of the delivery of the contract will attract a risk level of at least Very Low.

c. The Authority must submit this information to MOD Commercial as part of the procurement process: commercial staff cannot progress the competition / procurement without it.

d. Details of the Cyber Risk Profiles and, where the profile is not 'Not Applicable', the RAR number, will be included in the information sent out by MOD commercial to suppliers.

e. This process does not replace any contract specific security requirements which will continue to be addressed by a Security Aspects Letter.

5.2 Supplier Assurance Questionnaire

a. Any suppliers who wish to bid for the requirement will need to demonstrate their current level of compliance against the relevant controls set out in DEFSTAN 05-138. They will do this by logging on to Octavian and, citing the reference number, completing a supplier assurance questionnaire (SAQ) or linking to a previously completed return. The SAQ will only require them to answer those questions relevant to the level of risk of the contract they are bidding for, although they will have the option of choosing to test themselves against the full question set. The SAQ must be completed by an individual formally authorised to act on behalf of their Company and who may be held accountable for the submission.

b. The supplier will be able to choose the scope of their response, this can either be those parts of their system they will use to deliver this contract or it can be expanded to cover a wider network. This latter approach will increase the potential for re-use of a response but may make compliance at the higher levels of risk harder to achieve. Some suppliers may choose to complete a company-wide return to cover the lower risk levels and augment as required on a contract-by-contract basis at the higher levels of risk. All levels of risk above 'Not Applicable' require the supplier to hold a valid Cyber Essentials Certificate; Octavian will request the supplier to input their certificate number and certification body.

c. **Accredited networks.** A degree of information assurance is already delivered by using accredited networks. Suppliers who utilise accredited networks are still required to complete an SAQ but should include the accreditation details in the CIP and state why their network should be considered exempt from the controls appropriate to the applicable Cyber Risk Profile.

   i. **Standalone.** If MODII is processed solely on a standalone, accredited network the level of information assurance required by the MOD is delivered. In this scenario the contractor will complete an SAQ and submit a CIP with their proposal which contains their accreditation details, which is sufficient to claim compliance. This should, as a minimum, include: the accreditation authority, accreditation reference number and the date accreditation expires.

---

[1] 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).

ii. **Interconnected**. Where a contract will be delivered using an accredited network which has connectivity with other networks, the supplier must be compliant with the requirements of the DEFSTAN by completing an SAQ.

d. Compliance is the ideal outcome. Where suppliers do not comply but intend to in the future, or mitigate the risk of non-compliance, then a CIP is to be generated and signed-off in accordance with the instructions of para 7. In exceptional circumstances unmitigated risks are to be dealt with using the guidance and sign-off processes in paras 8 and 9.

e. When bids are received The Authority will confirm all suppliers have either:

i. Completed the SAQ and reached the required standard;

ii. Committed to doing so by an agreed date by submitting a CIP; or

iii. Committed to maintain alternative, appropriate controls described in a CIP which is acceptable to the MOD in accordance with the risk acceptance process for the CSM.

5.3 Flow-down

a. Where any sub-contracted element has access to, or creates MODII, the obligations of DEFCON 658 are to be flowed-down until the Cyber Risk Profile generated is 'Not Applicable'.

b. Items which involve neither the exchange nor creation of MODII may be grouped together and a RA performed to document the level as 'Not Applicable'; which infers MODII does not flow-down from this point. Whilst it is also possible to group other items with the same attributes and perform a risk assessment on these, caution must be exercised to ensure the attributes are the same and not just conveniently similar, to ensure the risk assessment process is robust.

c. The supplier will also complete the RAs on Octavian and, whilst each new RA will have its own unique RAR, Octavian will link that RAR to the master contract. Suppliers competing for a sub-contract will be required to either complete an SAQ using Octavian to demonstrate their compliance, or link to a previously completed return. The Authority agrees a contractor is entitled to rely upon the self-certification by a sub-contractor of compliance, using the CSM.

5.4 Visibility of Data

a. The default position will be for The Authority (whether MOD or a first tier supplier) to have visibility of the risk assessment they completed and the SAQ(s) linked to that risk assessment only.

b. There will be a small number of super-users in MOD who will have visibility of the whole supply chain. This will be used for three purposes:

i. To provide Management Information when requested e.g. how many contracts, what levels of risk, the percentage of compliance.

ii. To enable the identification of instances of non-compliance which do not appear to be under a risk acceptance regime.

iii. To enable the identification of suppliers who, through aggregation, may be carrying greater risk than the individual risk assessments would suggest. This enables the MOD to make informed decisions cognisant of their total risk picture.

5.5 Validity of Response

a. On an annual basis, after contract award, The Authority is to review the RA and, if the Cyber Risk Profile has increased, the supplier will need to complete the SAQ again. Where the MOD records a change in risk level then the tier one supplier will also be required to review the RA of any elements they have sub-contracted; where they record a change the tier two supplier will have to do likewise and so on, until there is no change.

b. Any material change within the supply chain will also require a refresh of the RA and, if the outcome shows a change in the risk level, a revised SAQ must be submitted. If The Authority (whether MOD or within the supply chain) changes the risk level during the contract this will be subject to a contract change being agreed and a formal contract amendment being issued. The supplier delivering that contract will then be expected to demonstrate compliance with the revised level of risk or, where this is not possible, put in place appropriate mitigations.

6. Risk Acceptance Process

a. If a supplier, regardless of their level in the supply chain, is unable to achieve the full controls required for compliance with the designated Cyber Risk Profile, a CIP may be used to either put a compliance plan in place or accept the risk of a supplier putting alternative or equivalent control measures in place. The following situations may require The Authority to agree a CIP:

i. a supplier has some controls in place but is unable to achieve the full controls designated to the level of cyber risk by Contract award;

ii. a supplier has alternative or equivalent mitigations in place; or

iii. a supplier/sub-contractor is unwilling to comply.

b. The above situations can occur not only at the start of the contract but also during the life of the contract where the Cyber Risk Profile changes due to a variation in the requirement or a revision to the control measures in DEFSTAN 05-138.

7. Cyber Implementation Plan (CIP)

a. The CIP allows the supplier to set out the steps they commit to taking to achieve compliance together with a timeframe for achievement. It should include detail on the current level of compliance, the planned measures to achieve compliance or the proposed mitigations for consideration. An indicative template is at Annex B.

b. Where The Authority agrees the measures are appropriate and do not result in unacceptable risk, they should agree the CIP. When a CIP is agreed the supplier will be treated on a par with suppliers achieving full compliance during the procurement and evaluation process.

c. Where a supplier is unable or unwilling to achieve compliance or has alternative measures in place, the CIP may also be used by the supplier to demonstrate to The Authority why they should consider accepting the risk of non-compliance.

d. Unless the supplier can prove an equivalent standard or there is a valid reason for non-compliance to the controls specified, acceptance of non-compliance should only be used in exceptional circumstances and assessed on case-by-case basis.

e. The agreed plan must form part of the final contract award or amendment. The Authority must periodically review the plan to ensure progress is being made within the agreed timeframe.

8. MOD Acceptance and Agreement of a CIP

a. The level of approval required for acceptance of risk on top-tier contracts will depend on the designated Cyber Risk Profile and ranges from The Authority (i.e. the MOD project team in this case) to the Senior Information Risk Owner (SIRO). The levels are set out below.

i. For contracts assessed as carrying a Very Low or Low cyber risk, the risk can be accepted by The Authority (i.e. the MOD project team in this case) / contract SRO and notified to the Major Business Unit / Front Line Command SIRO.

ii. For Moderate risk contracts, the risk can only be accepted by a TLB Accreditor / Principal Security Advisor (PsyA) on behalf of the Major Business Unit / Front Line Command SIRO.

iii. For High risk contracts, the risk can only be accepted by DAIS (Defence Assurance and Information Security) accreditors on behalf of the MOD's SIRO (with escalation to the MOD's SIRO as required).

c. The acceptance of risk should be guided by the Departmental Risk Appetite statement, issued by the MOD's SIRO, which will be updated annually.

d. The acceptance of risk by the MOD will be guided by 2016DIN02-004 which states the MOD's Risk Appetite statement, issued by the MOD's SIRO.

9. Supply Chain Acceptance and Agreement of a CIP

a. For contracts for all Cyber Risk Profiles a CIP may be accepted by the higher tier supplier if they are satisfied the risk is being appropriately mitigated. All such decisions must be notified to the next higher tier buyer and ultimately to the MOD using the RAR as a unique reference.

b. Where there are no mitigations in place or the higher tier supplier is not satisfied the risk is appropriately mitigated:

i. For Very Low and Low Cyber Risk Profiles the higher tier supplier can accept the risk (notifying The Authority within the MOD of this acceptance).

ii. For Moderate Cyber Risk Profiles, the risk can only be accepted by the MOD TLB / FLC / Major Business Unit SIRO / PsyA.

iii. For High Cyber Risk Profiles, any decisions on risk acceptance must be made in consultation with MOD DAIS.

c. Regardless of the level of acceptance, the existence of risk must be recorded on Octavian, together with the acceptance of the CIP.

d. Where the Cyber Risk Profile changes during the life of the contract, the CIP may need to be re-visited. Any changes should be agreed in accordance with the levels above.

Annex A Cyber Risk Profiles

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

Every MOD requirement must be subject to a Risk Assessment and have one of these five profiles assigned. The Cyber Risk Profiles are related to appropriate controls detailed in this Annex.

a) Any contract not involving MODII will be deemed to carry no cyber risk and assessed as 'Not Applicable'.

b) 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.

Not Applicable

2. The Not Applicable outcome does not require specific cyber control measures although it is recommended all suppliers, as a matter of good practice, should achieve compliance with the Cyber Essentials Scheme.

Cyber Risk Profile Very Low

3. The Very Low Cyber Risk Profile 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 Table 1. For further information search 'DCPP' on the GOV.UK website.

CSM Very Low Cyber Risk Profile Requirements
Info-Cyber Systems Security
VL.01 Maintain Cyber Essentials Scheme certification.

Table 1 – DCPP Cyber Risk Profile – Very Low

Cyber Risk Profile Low

4. The Low Cyber Risk Profile 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 Table 2. For further information search 'DCPP' on the GOV.UK website.

CSM Low Cyber Risk Profile Requirements
Governance
L.01 Define and assign information security relevant roles and responsibilities.
L.02 Define and implement a policy which addresses information security risks within the supply chain.
Security Culture and Awareness
L.03 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.04 Define employee (including contractor) responsibilities for information security.
L.05 Define and implement a policy to provide employees and contractors with information security training.
Information Asset Security
L.06 Define and implement a policy for ensuring sensitive information is clearly identified.
L.07 Define and implement a policy to control access to information and information processing facilities.
Info-Cyber Systems Security
L.08 Maintain Cyber Essentials Scheme Plus Certification.
L.09 Define and implement a policy to control the exchanging of information via removable media.
L.10 Define and implement an information security policy, related processes and procedures.
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.
Personnel Security
L.13 Define and implement a policy for verifying an individual’s credentials prior to employment.
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.
Security Incident Management
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.

Table 2 – DCPP Cyber Risk Profile – Low

Cyber Risk Profile Moderate

5. The Moderate Cyber Risk Profile 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 Table 3. For further information search 'DCPP' on the GOV.UK website.

CSM Moderate Cyber Risk Profile Requirements	
Security Governance	
L.01 Define and assign information security relevant roles and responsibilities.	
L.02 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.	
Security Culture and Awareness	
L.03 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.04 Define employee (including contractor) responsibilities for information security.	**M.02** Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.
L.05 Define and implement a policy to provide employees and contractors with information security training.	
Information Asset Security	
L.06 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.	
L.07 Define and implement a policy to control access to information and information processing facilities.	**M.06** Ensure the organisation has identified asset owners and asset owners control access to their assets.
Info-Cyber Systems Security	
L.08 Maintain Cyber Essentials Scheme Plus Certification.	
L.09 Define and implement a policy to control the exchanging of information via removable media.	
L.10 Define and implement an information security policy, related processes and procedures.	
L.11 Record and maintain the scope and configuration of the information technology estate.	
M.07 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.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	
L.12 Define and implement a policy to manage the access rights of user accounts.	**M.09** Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.10 Define and implement a policy to control remote access to networks and systems.	

<table>
<tr><th colspan="2">CSM Moderate Cyber Risk Profile Requirements</th></tr>
<tr><td colspan="2">M.11 Define and implement a policy to control the use of authorised software.</td></tr>
<tr><td colspan="2">M.12 Define and implement a policy to control the flow of information through network borders.</td></tr>
<tr><td colspan="2">M.13 Define and implement a policy to maintain the confidentiality of passwords.</td></tr>
<tr><th colspan="2">Personnel Security</th></tr>
<tr><td>L.13 Define and implement a policy for verifying an individual’s credentials prior to employment.</td><td>M.14 Define and implement a policy for applying security vetting checks to employees.</td></tr>
<tr><td colspan="2">L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.</td></tr>
<tr><td colspan="2">L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.</td></tr>
<tr><td colspan="2">M.15 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.</td></tr>
<tr><td colspan="2">M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.</td></tr>
<tr><th colspan="2">Security Incident Management</th></tr>
<tr><td colspan="2">L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.</td></tr>
</table>

Table 3 – DCPP Cyber Risk Profile – Moderate

Cyber Risk Profile High

6. The High Cyber Risk Profile 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 Table 4. For more information search 'DCPP' on the GOV.UK website.

CSM High Cyber Risk Profile Requirements	
Security Governance	
L.01 Define and assign information security relevant roles and responsibilities.	
L.02 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.	
Security Culture and Awareness	
L.03 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.04 Define employee (including contractor) responsibilities for information security.	**M.02** Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.
L.05 Define and implement a policy to provide employees and contractors with information security training.	
Information Asset Security	
L.06 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.	
L.07 Define and implement a policy to control access to information and information processing facilities.	**M.06** Ensure the organisation has identified asset owners and asset owners control access to their assets.
Info-Cyber Systems Security	
L.08 Maintain Cyber Essentials Scheme Plus Certification.	
H.01 Maintain patching metrics and assess patching performance against policy.	
H.02 Ensure wireless connections are authenticated.	
L.09 Define and implement a policy to control the exchanging of information via removable media.	
L.10 Define and implement an information security policy, related processes and procedures.	
L.11 Record and maintain the scope and configuration of the information technology estate.	
M.07 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.08 Define and implement a policy to monitor	**H.03** Deploy network monitoring techniques

CSM High Cyber Risk Profile Requirements	
network behaviour and review computer security event logs for indications of potential incidents.	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.09** Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.10 Define and implement a policy to control remote access to networks and systems.	
M.11 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.12 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.
M.13 Define and implement a policy to maintain the confidentiality of passwords.	
H.08 Undertake administration access over secure protocols, using multi-factor authentication.	
H.09 Design networks incorporating security countermeasures, such as segmentation or zoning.	
H.10 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.13 Define and implement a policy for verifying an individual's credentials prior to employment.	**M.14** Define and implement a policy for applying security vetting checks to employees.
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.	
M.15 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.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	
Security Incident Management	
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.	
H.11 Proactively verify security controls are providing the intended level of security.	
H.12 Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis	

Table 4 – DCPP Cyber Risk Profile – High

Annex B CSM - Cyber Implementation Plan Template

Contract title	
MOD contract number:	
CSM Risk Acceptance Reference:	
CSM Cyber Risk Profile:	
Name of Supplier: (To be shared with the MOD only)	
Current level of Supplier compliance:	
Reasons unable to achieve full compliance:	
Measures planned to achieve compliance / mitigate the risk with dates:	
Anticipated date of compliance / mitigations in place:	
Risk Accepted and by whom:	Yes / No
Notified (If applicable):	Yes / No
Decision recorded on Octavian:	Yes / No
Name	
Position	
Date	

Annex C MOD Identifiable Information

1. For the purpose of the DCPP, the definition of MOD Identifiable Information is:

   All Electronic Information (as defined in DEFCON 658) 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.

2. The list of illustrative criteria below is a guide of the factors to consider when deciding if a requirement is within the scope of MOD Identifiable Information. It is not a definitive list and one must consider each requirement on a case-by-case basis, and adopt a reasonable, pragmatic and proportionate approach when deciding what is classed within scope.

3. Information will not be considered to be MOD Identifiable Information where it is already in the public domain, other than by a breach of any contractual or common law duty of confidentiality.

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 A.2, A.3 & A.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	DEFCON 658

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 A.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 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.
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 .
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, 2017DIN02-006, Industry Security Notice 2017/04 and at Annex C. (DEFCON 658 remains the authority on defining MODII).
Octavian	Octavian is the online tool developed in partnership with industry and delivered by a third-party, which is utilised for the completion of RAs and SAQs. Certain users within the MOD have super-user access and are able to interrogate the data for business improvement and risk management purposes.
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).

Abbreviations

Abbreviation	Description
APT	Advanced Persistent Threats
CES	Cyber Essentials Scheme
CES+	Cyber Essentials Scheme Plus
CIP	Cyber Implementation Plan
CSM	Cyber Security Model
DCPP	Defence Cyber Protection Partnership
MODII	MOD Identifiable Information
RA	Risk Assessment
RAR	Risk Assessment Reference
SAQ	Supplier Assurance Questionnaire
SIRO	Senior Information Risk Owner

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

DStan Helpdesk

Tel: +44 (0) 141 224 2531

Fax: +44 (0) 141 224 2503

Internet e-mail: enquiries@dstan.mod.uk

File Reference

The DStan file reference relating to work on this standard is D/DStan/24/138.

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.