Defence Cyber
Protection Partnership

Defence Cyber Protection Partnership

Cyber Security Model
Industry Buyer and Supplier Guide

June 2018

Introduction

1. The purpose of this guide is to provide industry with information relating to the Defence Cyber Protection Partnership's (DCPP) Cyber Security Model (CSM) (shown diagrammatically at Annex A). This version 2.1 of the Buyer and Supplier Guide, issued in June 2018. Please note, the CSM is has been applied beyond the first tier of the supply chain since October 2017. The CSM is a risk-based approach to protecting MOD Identifiable Information (MODII) as it is passes down the supply chain. A definition of MODII is at Annex B.

0. The CSM enforces controls for the protection of MODII and whilst this protection extends to personal information, those seeking to place contracts involving the generation, handling or processing of HR data should be aware of the MOD's restrictions on off-shoring (storing information on electronic systems outside of the UK). Guidance will be available from the MOD Authority via Defence Instructions and Notices 2016DIN02-004.

1. From **1st October 2017,** all new MOD contracts involving the electronic exchange of MODII must include a Risk Assessment using the DCPP's online tool (Octavian). If MODII flows-down the supply chain then each supplier must, in turn, complete a Risk Assessment. This is a change from the previous process which was implemented on 1st April 2017, for all new MOD contracts but which only applied to the first tier of the supply chain.

Key documents

2. The two key MOD policy documents supporting this process are the Cyber Security Commercial Policy Statement[1] (access via MODnet) and DEFSTAN 05-138[2]. Key to the CSM is DEFCON 658, which is a contract condition.

Background

2. HMG and industry developed the Cyber Essentials Scheme[3] which is the standard selected by the MOD and industry to ensure all organisations working with the MOD have basic cyber security measures in place. The Cyber Essentials Scheme (CES), launched across Government on 5 June 2014, has been a mandatory requirement for suppliers with contracts involving sensitive or personal information since 1 October 2014.

3. The MOD initially had an exemption from the CES. From 1 January 2016, all MOD suppliers were required to have Cyber Essentials for new contracts involving the transfer, or generation of, MODII. DEFCON 658 remains the authority for the definition of MODII. A definition of MODII is at Annex B.

4. As an extension of the Government's CES the MOD, working together with industry and Other Government Departments, developed a more robust CSM under the umbrella of the DCPP. The DCPP is improving Defence's supply chain security, improving its understanding of where the cyber risks are.

5. The model, outlined below, was implemented in new Defence contracts from 3 April 2017 to Tier One contracts only and applied down the supply chain from 1 October 2017. This process dovetails with the Risk Balance Case (RBC) process and is not be considered in isolation.

The CSM Process

6. The three main components of the CSM are:

1. A Risk Assessment (RA) is conducted by The Authority to evaluate the degree of cyber risk to a specific contract and establish a Cyber Risk Profile;

2. A Supplier Assurance Questionnaire (SAQ), is completed by suppliers who wish to be

1 http://aof.uwh.diif.r.mil.uk/aofcontent/tactical/toolkit/downloads/cyber/cyber_cps.pdf

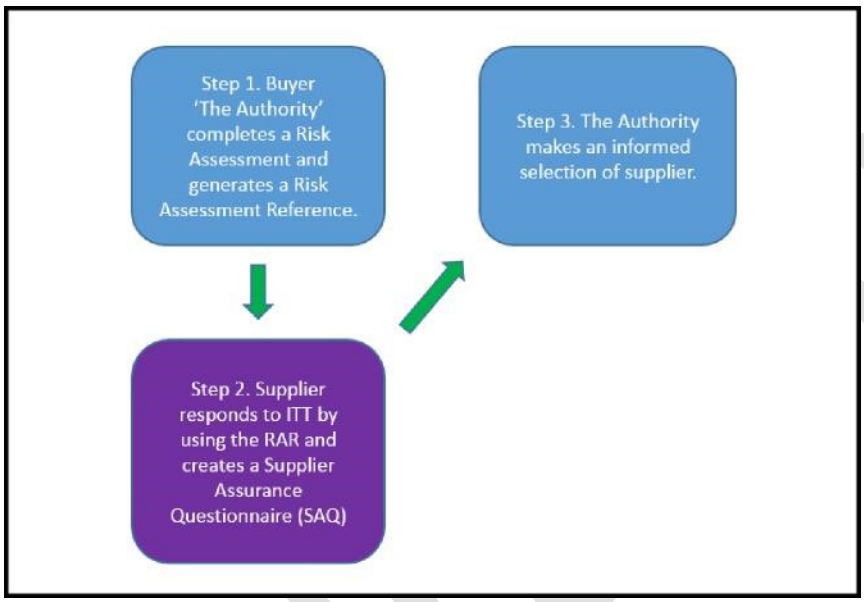
2 http://dstan.uwh.diif.r.mil.uk/standards/defstans/05/138/00000100.pdf

3 https://www.cyberessentials.ncsc.gov.uk/

considered for that contract;

3. An evaluation of the SAQs including supporting evidence, such as a Cyber Implementation Plan (CIP), by The Authority. This is used in the contract award process.

Figure 1. **The Cyber Security Model**



Cyber Security Model in Detail

10. The following paragraphs give more detail on the three-stage process outlined above.

- For all new requirements, it is mandatory for The Authority to complete an RA using the online tool. This top-level assessment looks at the type of MODII generated and the potential harm caused by exposure of this information. A workflow diagram of the questions is available in the Risk Assessment Workflow guide[4].

- The RA will generate the Cyber Risk Profile and a unique Risk Assessment Reference (RAR). DEFSTAN 05-138 details a series of controls for each Cyber Risk Profile necessary for a supplier to implement to receive and handle MODII.

- The RAR is used by potential suppliers when completing an SAQ responding to an ITT. **Early notification** gives potential suppliers more time to achieve compliance with the Cyber Risk Profile.

- It is essential the SAQ is completed by all potential suppliers bidding for a contract using Octavian, the online tool. Suppliers must input the RAR associated with the contract and answer specific questions related to the Cyber Risk Profile for that contract. A workflow diagram of the questions is in the Supplier Assurance Questionnaire Workflow guide[5].

- If a potential supplier fails to demonstrate compliance with their allocated Cyber Risk Profile, they have an option to commit to achieving compliance at an agreed date by submitting a Cyber Implementation Plan (CIP) as part of their tender submission. The CIP, as detailed in DEFSTAN 05-138, provides evidence as to how and when potential suppliers will achieve compliance.

- Where The Authority agrees the measures identified in the CIP are appropriate and do not result in an unacceptable risk, they must agree the CIP before contract start date and monitor the supplier's compliance as part of their usual project management activities. The

4 https://www.gov.uk/government/publications/supplier-cyber-protection-service-risk-assessment-workflow

5 https://www.gov.uk/government/publications/supplier-cyber-protection-service-supplier-assurance-questionnaire-workflow

level of approval required for acceptance of risk will depend on the designated Cyber Risk Profile and ranges from the Project Manager to the MOD's Senior Information Risk Owner. Direction on the CIP and acceptance of risk is in DEFSTAN 05-138.

11. From 1st October 2017, the CSM applied to all suppliers down the supply chain, processing MODII. The prime contractor will complete an RA for any intended sub-contracts. The newly generated RAR is then distributed to potential sub-contractors who will complete an SAQ to demonstrate their compliance. The prime contractor will consider the SAQ response as part of their contract award process and agree a CIP as necessary. This process proceeds down the supply chain up to a point where MODII is neither moved, saved, or retrieved electronically.

Managing Cyber Risk

12. Cyber risk should be managed at the various stages of the procurement cycle including:

a. Requirement setting. At each tier of the supply chain, The Authority[6] will conduct a Risk Assessment to assess the level of cyber risk, as defined in DEFSTAN 05-138 in all contracts they place. If the requirement or supply chain changes at any point during the life of the contract, a new **RA** must be conducted to assess change to the Cyber Risk Profile.

b. Contract terms and conditions. The CSM will be managed by including contract terms and conditions in the form of DEFCON 658 or equivalent terms in all contracts together with an associated note stating the allocated Cyber Risk Profile and referencing any agreed Cyber Implementation Plan (CIP), as appropriate. The CIP should become a schedule to the contract, where one is agreed.

c. Contract management. All suppliers throughout the supply chain must complete an annual reassessment of their SAQ to confirm continued compliance with the Cyber Risk Profile. Suppliers must ensure they comply with the contract's conditions regarding record keeping and audit and make available all records associated with compliance to DEFCON 658 on request.

d. Risk management. The CSM will inform the existing RBC process and whilst it is recognised completion of this process is additional work, it is essential to understand the cyber risks facing Defence so they are managed appropriately.

13. **Risk Acceptance**

a. **MOD Acceptance and Agreement of Risk**. Guidance on MOD Acceptance and Agreement of a CIP is in DEFSTAN 05-138, para 8. A CIP enables a supplier to evidence they are delivering the same degree of information assurance as required by DEFSTAN 05-138 in that they are doing so by enforcing different, but equivalent controls. If The Authority considers the supplier's controls to be not as effective as those in DEFSTAN 05-138 this creates a degree of risk. The level of risk must communicated and potentially accepted according to the guidance in DEFSTAN 05-138, summarised below.

6 The Authority is the role which determines the Cyber Risk Profile appropriate to a contract and notifies the Supplier of this profile, and any changes, as soon as reasonably practicable. Where the contract is between the MOD and the supplier the MOD is The Authority; where the contract is between a supplier to the MOD and a sub-contract, the supplier becomes The Authority.

Cyber Risk Profile	Risk Accepter (Accountable)	Informed of risk acceptance
N/A	N/A	N/A
Very Low	The Authority (MOD) or MOD contract SRO	Major Business Unit / Front Line Command SIRO
Low	The Authority (MOD) or MOD contract SRO	Major Business Unit / Front Line Command SIRO
Moderate	TLB Accreditor / Principal Security Advisor (PsyA)	Major Business Unit / Front Line Command SIRO
High	Defence Assurance and Information Security accreditor	MOD SIRO

Industry Acceptance and Agreement of a CIP. Guidance on Industry Acceptance and Agreement of a CIP is in DEFSTAN 05-138, para 9. A CIP enables a supplier to evidence they are delivering the same degree of information assurance as required by DEFSTAN 05-138 in that they are doing so by enforcing different, but equivalent controls. If the buyer considers the supplier's controls to be not as effective as those in DEFSTAN 05-138 this creates a degree of risk. The level of risk must be communicated and potentially accepted according to the guidance in DEFSTAN 05-138, summarised below.

Cyber Risk Profile	Risk Accepter (Accountable)	Informed of risk acceptance
N/A	N/A	N/A
Very Low	Higher tier supplier	The Authority (MOD) or MOD contract SRO
Low	Higher tier supplier	The Authority (MOD) or MOD contract SRO
Moderate	MOD TLB / FLC / Major Business Unit SIRO / PsyA	MOD TLB / FLC / Major Business Unit SIRO / PsyA
High	Defence Assurance and Information Security accreditor	Defence Assurance and Information Security accreditor

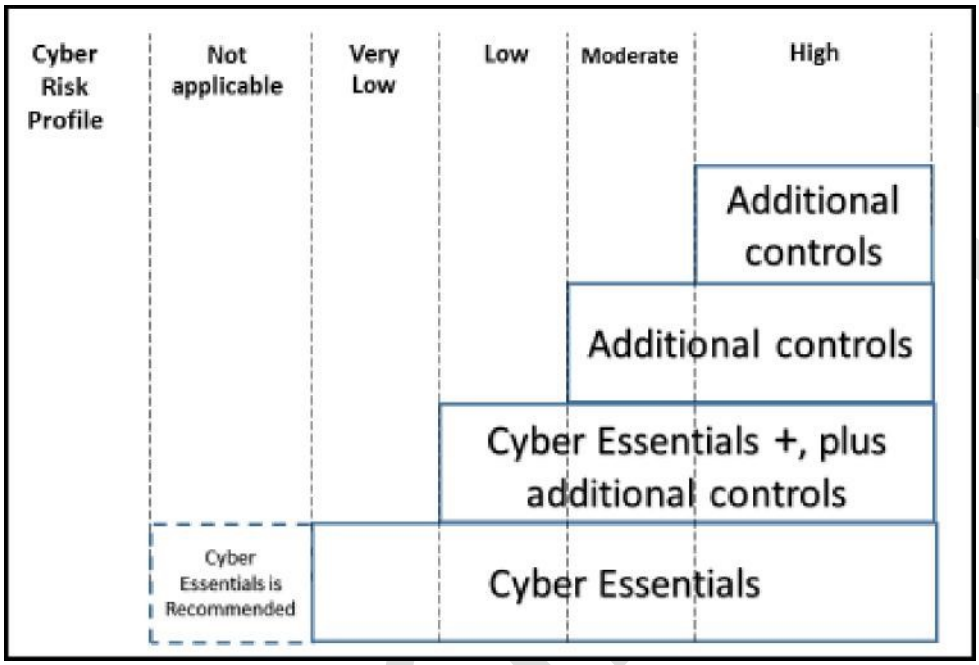
Cyber Risk Profiles

14. DEFSTAN 05-138 defines cyber risk as "the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise". The Authority is responsible for assessing the level of cyber risk for each requirement by completing an RA and, in doing so, answering a series of questions relating to the requirement which will result in a Cyber Risk Profile. The RA is completed using Octavian. The Cyber Risk Profiles are designed to

be proportionate to the level of risk associated with the contract which may change at each level of the supply chain. This ensures smaller companies at lower levels of the supply chain only

require the controls necessary to protect the level of risk associated with their specific contract. This was a key factor in the approach taken by the DCPP to ensure the Defence supply chain remains as open as possible.

Figure 2 – **Cyber Risk Profiles and Commensurate Control Summary**



15. Where the requirement does not involve the transfer of MODII the RA will result in a 'Not Applicable' outcome. This means Cyber Essentials certification is recommended but not mandated by the MOD.

16. Below is a list of the Cyber Risk Profiles. Full details on the controls are in DEFSTAN 05-138 and Octavian.

- N/A- No action required. Although MOD policy is for all suppliers to have Cyber Essentials certification as a minimum.
- Very Low - Cyber Essentials certification.
- Low - Cyber Essentials Plus certification, plus additional controls.
- Moderate - All the requirements of 'Low' and additional controls.
- High – All the requirements of 'Moderate' and additional controls.

17. Each of the Cyber Risk Profiles mandates the controls suppliers must implement to demonstrate compliance. The higher the risk profile, the greater the controls required.

18. The Cyber Risk Profile is designed to be proportionate to the degree of MODII being exchanged and will, in most instances, decrease at each level of the supply chain. One should not assume a prime contractor operating with a High Cyber Risk Profile, will place all sub-contracts at

high. This ensures SMEs are not disadvantaged by needing to have High controls, if the extent of MODII exchange is minimal.

19. The Authority must reassess the Cyber Risk Profile if there is a material change to the requirement or a change to the supply chain during the life of the contract. Any changes to the Cyber Risk Profile must go through a contract change control process and be subject to formal contract amendment. The CIP is to be updated as necessary, and agreed between the parties.

20. **Two-factor authentication**

a. Security requirements mean two-factor authentication (2FA) is needed to both register and access the service. This requires a combination of a pin number, defined by the user at registration, and a second code provided by a second authentication method. There are several options for this method to facilitate different users' requirements:

(1) A code given by text message sent to a mobile phone number, which is provided by the user at registration;

(2) A code given by a mobile app, which is obtained by contacting service support;

(3) A code given by a hardware token associated with the user account, obtained by contacting service support; and

(4) A code given over the phone, following the user contacting service support and giving characters from their security question.

21. **User identity verification.** For RAs deemed to have a Cyber Risk Profile of Moderate or above, those wishing to respond with an SAQ need to verify their identity. Users will be notified of this requirement through Octavian, and will be required to contact NQC's service support and provide two forms of identity verification, the list of acceptable forms can be seen in Annex E. Once a user's account has been verified their account will be permanently able to respond to RAs with Moderate and above Cyber Risk Profiles. In 2018 Verify[7] will be implemented to enable identity assurance for UK citizens who are submitting an SAQ in response to a Cyber Risk Profile of Moderate or above.

Document updates

22. DEFCON 658 was updated to Edition 10/17 on the Commercial Toolkit, accessible via the Defence Gateway at the start of October 2017. DEFSTAN 05-138 2017 was issued on 28th September 2017 and will be reviewed and updated annually thereafter. Changes to the DEFSTAN were signposted in ISN2017/06[8].

23. Interested parties are recommended to join the DCPP Group on the Cyber Security Information Sharing Partnership (CiSP) where future changes to the DEFSTAN's controls will be communicated and discussed. The CiSP is accessible via https://www.ncsc.gov.uk/cisp.

Supplier Selection

24. MOD prime contract suppliers are alerted to the Cyber Risk Profile through the Contract Notice or ITT documentation, which will inform them of the security controls associated with the contract. All potential suppliers invited to tender must complete the SAQ using Octavian. The ITT will specify the unique RAR from Octavian, which will allow the supplier to complete their SAQ.

25. Suppliers should be aware of the need for 2FA for the Cyber Risk Profiles of Moderate and High and are to follow the steps in Octavian to request access.

26. Where the prime contractor intends to subcontract any element of the requirement they must assess the Cyber Risk Profile of the subcontract and, if the Cyber Risk Profile is higher than 'Not Applicable', require their supplier to complete a SAQ. If the prime contract is assessed as High, ~~the Cyber Risk Profile of the~~ subcontract is not automatically assessed as High but will be

7 https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

8 https://www.gov.uk/government/publications/industry-security-notices-isns

dependent on the level of MODII transferred against the subcontracted requirement. This process will be flowed down the whole supply chain until a 'Not Applicable' Cyber Risk Profile is achieved.

27. As with the prime contract, the subcontractor must have appropriate cyber security controls in place at contract placement or agree a CIP with the prime contractor.

Supplier Evaluation

28. Where the Cyber Risk Profile is higher than 'Not Applicable' The Authority must include equivalent terms to DEFCON 658 and the allocated Cyber Risk Profile in the terms and conditions.

29. If a supplier is not able to meet the security controls required by the contract start date, the supplier should submit a CIP with their tender detailing the steps they would take to meet the necessary controls, together with associated timescales, details of any equivalent standards they have, or reasons why they are unable to comply. The CIP and supporting documents will be considered as part of the extant RBC process. Detail on the CIP acceptance process is in DEFSTAN 05-138 and guidance on what is expected in a CIP is at Annex D.

Contract Terms and Conditions

3. Where The Authority has identified a Cyber Risk Profile higher than 'Not Applicable', The Authority must include equivalent terms to DEFCON 658 on the resultant contract together with the following note stating the allocated Cyber Risk Profile:

> "Further to the Cyber Security Condition the Cyber Risk Profile of the Contract is [ ], as defined in DEFSTAN 05-138."

30. An agreed CIP will become a schedule to the contract. The Authority must ensure the supplier meets the agreed timescales within the CIP for implementation and brings to their supplier's attention at the earliest opportunity any issues concerning its supply chain relating to the necessary cyber controls. Once the contract is in place the prime contractor is expected to alert the MOD to any issues or changes in its supply chain which may affect the existing cyber risk profile.

Contract Management

31. If there is a material change to the requirement The Authority must re-complete the RA. If the Cyber Risk Profile changes at any point during the life of the contract this must be the subject of a formal contract amendment.

32. The Authority must ensure the supplier completes the SAQ on an annual basis to ensure continued compliance with the security controls. Octavian will provide notification to account holders to prompt them to take this action.

33. The Authority must also ensure, where the supplier has subcontracted an element of the requirement they are managing the cyber risk in their supply chain, including requiring the sub-contractor to complete an annual SAQ.

34. The Authority must complete a new RA for any change of supplier during the life of the contract and require the proposed, new sub-contractor to complete a SAQ.

35. The MOD intends to work jointly with industry to improve the management of cyber risk and increase awareness across Defence to assure the MOD's capability. By employing the CSM, all suppliers are encouraged to share lessons learnt so the MOD and industry can react to changes and improve their cyber resilience.

36. Attention is drawn to the Cyber Security Information Sharing Partnership (CiSP). This is a joint industry and government initiative to exchange cyber threat information. This is done in real time, using a secure, confidential and dynamic environment increasing situational awareness and reducing the impact of cyber threats on UK businesses. Suppliers are recommended to join the DCPP Group on the CiSP (see www.ncsc.gov.uk/cisp).

37. Cyber security is an ever-evolving field. For this reason the CSM and the Cyber Risk Profiles in DEFSTAN 05-138 may change. Changes will be managed in accordance with the DEFSTAN change process at Annex C. If the Supplier suffers or will suffer any delay or incurs additional cost

as a result of a change to the DEFSTAN, the Supplier may seek a reasonable adjustment to the contract price and / or an extension to the time for compliance with such revisions which should be dealt with as a contract amendment.

38. Some of the rights contained in DEFCON 658 continue after contract completion. At contract end, MOD will review the information transferred to the prime in relation to the contract. This is to check if is still considered MODII, and therefore continued to be covered by DEFCON 658. DEFCON 658 remains the authority for the definition of MODII; for convenience, the definition is at Annex B. The Authority and suppliers through the supply chain will need to conduct the same review of their own contracts.

Cyber Incidents

39. DEFCON 658 includes provisions for termination of contract in relation to the CSM. The Authority must not, however, automatically terminate the contract, either whole or in part, or claim damages for a cyber-attack that occurred despite the supplier complying with the CSM process. The same applies to a cyber-attack suffered by a lower tier sub-contractor.

40. A breach of DEFCON 658 is not defined as a cyber incident per se, but is defined as a breach of the process and standards mandated in the CSM.

41. In accordance with DEFCON 658, the Supplier must report, as soon as they know or have reasonable grounds to believe, a cyber incident has occurred. The Supplier is to provide full details of the circumstances of the incident and any mitigation measures they have taken or intend to take. The Authority should consider each incident on a case-by-case basis and consult the Supplier before deciding on the appropriate action to take.

42. Any resultant action must be reasonable and proportionate to the Cyber Risk Profile of the contract and the relevant RBC.

Further Information

43. More information on Cyber Essentials and the CSM is available from the following sources:

a. Via the NCSC for the Cyber Essentials Scheme[9] and GOV.UK for further information the DCPP[10].

b. The Lancaster University report[11] on the effectiveness of the Cyber Essentials Scheme.

c. Advice on cyber security for small and large businesses is available here: https://www.gov.uk/government/collections/cyber-security-guidance-for-business

d. DEFSTAN 05-138[12] – Cyber security controls for Defence Suppliers.

e. The Cyber Security Commercial Policy Statement and DEFCON 658[13] on the MOD Commercial Toolkit via the Defence Gateway[14].

f. There is a DCPP Group on the CiSP, which is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business. Further information is at https://www.ncsc.gov.uk/cisp.

g. The DCPP has a group on LinkedIn[15], which all are welcome to join.

9 https://www.cyberessentials.ncsc.gov.uk/

10 https://www.gov.uk/government/collections/defence-cyber-protection-partnership

11 https://nms.kcl.ac.uk/jose.such/pubs/SCC-2015-02-CS-Controls-Effectiveness.pdf

12 https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138

13 https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

14 https://defencegateway.mod.uk/home/

15 https://www.linkedin.com/groups/8351197

h. Defence Procurement has a new Twitter handle @DefenceProc, which all are welcome to follow.

i. Excellent education sources on cyber security are available, free of charge, at https://www.futurelearn.com/courses/introduction-to-cyber-security.

Annexes:

A. The Cyber Security Model

B. MOD Identifiable Information

C. DCPP CSM Change Control Process

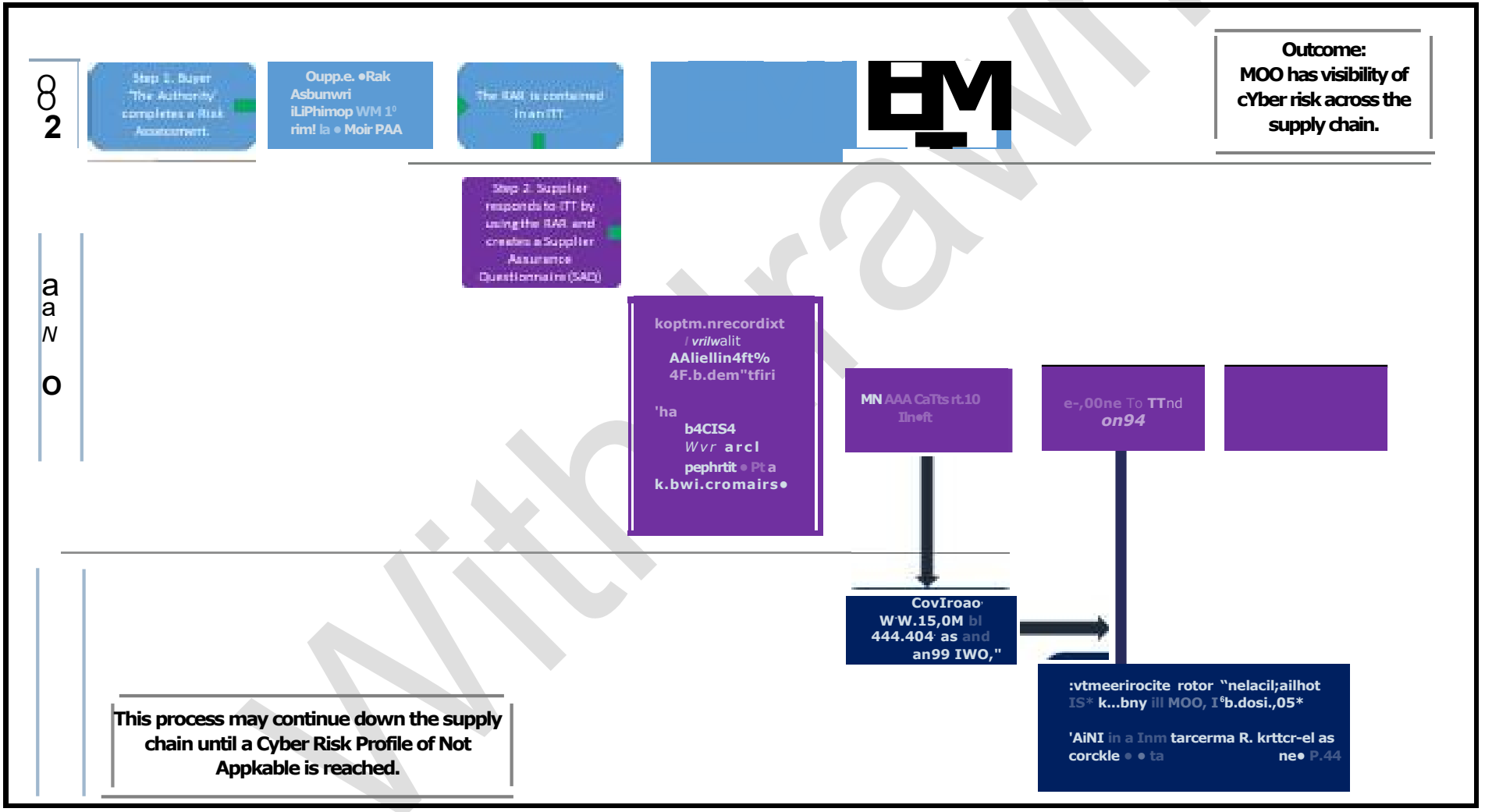
D. Guidance on Submission of a Cyber Implementation Plan (CIP)

E. Documents Acceptable to Validate a User's Identity

F. Definitions and Abbreviations

Annex A

The Cyber Security Model


Step 1. Buyer The Authority completes a Risk Assessment.
Oupp.e. •Rak Asbunwri iLiPhimop WM 1° rim! la • Moir PAA
The RAR is contained in an ITT
Step 2. Supplier responds to ITT by using the RAR and creates a Supplier Assurance Questionnaire (SAQ)
koptm.nrecordixt / vrilwalit AAliellin4ft% 4F.b.dem"tfiri
'ha b4CIS4 Wvr arcl pephrtit • Pt a k.bwi.cromairs•
MN AAA CaTts rt.10 Ilnoft
e-,00ne To TTnd on94
CovIroao· W·W.15,0M bl 444.404· as and an99 IWO,"
:vtmeerirocite rotor "nelacil;ailhot IS* k...bny ill MOO, I⁶b.dosi.,05*
'AiNI in a Inm tarcerma R. krttcr-el as corckle • • ta ne• P.44
Outcome: MOO has visibility of cYber risk across the supply chain.
This process may continue down the supply chain until a Cyber Risk Profile of Not Appkable is reached.

Annex B

MOD Identifiable Information

1. 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, otherwise 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))	MOD Statements of Work (SOW)
Contract Number (unless specified in a contract specific SAL)	MOD Technical Requirements
Quantity and Delivery schedule (unless specified in a contract specific SAL)	MOD Acceptance and Test Parameters (and corresponding results)
Delivery Address (unless specified in a contract specific SAL)	MOD Drawings and documents
DEFCONs and Def Stans	MOD Interface Drawings / Documents
Standard Contract Text	Documents marked as OFFICIAL SENSITIVE or with any form of handling instruction
AQAP Quality Conditions	Anything covered by a SAL (which always take precedence)
Standard Industry / Commercial accreditation (e.g. BS Standards)	Foreground Intellectual Property
Company Proprietary Information	Personal Data / Medical records and all information covered by the Data Protection Act (DPA)
COTS (Commercial Off The Shelf) product information	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.

Annex C

DCPP Change Control Process

1. Cyber threats change and the DCPP has a remit to maintain an 'evergreen' approach to cyber resilience, overseen by the DCPP's Executive Group. The processes outlined below are used to amend and update the CSM and applicable controls.

Changes to the Cyber Security Model

2. Any changes to the CSM process, for example the Risk Assessment or Supplier Assurance Questionnaire, will be consulted through the DCPP's Measurements and Standards Group and updated on Octavian.

MOD Changes to the Risk Assessment

3. Where there has been a materiel change to the contract requirement and the MOD requires the cyber controls to be met at a higher level, this will be formally dealt with through the contract change procedure and a formal contract amendment. The Authority will need to reflect this change throughout the supply chain as appropriate.

Changes to Defence Standard 05-138

4. Changes to the DEFSTAN will be consulted and agreed through the DCPP's Measurements and Standards Group.

5. Notification to industry of changes to the DEFSTAN will be through an Industry Security Notice and the DCPP Group on the CiSP.

Annex D

Guidance on Submission of a Cyber Implementation Plan (CIP)

The CIP allows flexibility in the delivery of assurance of information by enabling suppliers to evidence the controls they are implementing, or will implement, to deliver an equivalent degree of protection of MODII to match the controls designated in the DEFSTAN 05-138.

The submission of a CIP is a commitment by a supplier to enforce the controls referred to in that document. The controls may be enforced at the time of the CIP's submission or the supplier may select to implement the controls at a future date. The CIP is a contractually binding document, to be considered as part of the supplier's submission.

What should a CIP look like?

Not acceptable

ACME Manufacturing does not hold Cyber Essentials certification but does hold ISO27001.

Why is this not acceptable?

First, the CIP does not follow the CIP template in DEFSTAN 05-138.

Second, ISO27001 applies to systems which are 'in-scope'. The award of an ISO27001 certification does not automatically include the systems which will process MODII. The controls in ISO27001 do not all equate to those mandated in DEFSTAN 05-138 and it is this level of detail which is required to ensure appropriate controls are in place.

Acceptable

The proposed template is in DEFSTAN 05-138 at Annex B and this template should be used to commence a CIP.

Example 1

Contract title	Stealth Spinner Widget
MOD contract number:	123ABC
CSM Risk Assessment Reference:	QWEASDZXC123
CSM Cyber Risk Profile:	Very Low
Name of Supplier: (To be shared with the MOD only)	Acme Manufacturing
Current level of Supplier compliance:	Very Low
Reasons unable to achieve full compliance:	Acme Manufacturing holds ISO27001 for part of its enterprise IT systems but not those

Contract title	Stealth Spinner Widget
	which will manage MODII if the contract is awarded. Acme Manufacturing does not hold Cyber Essentials and will not gain that certification as sufficient controls are in place to overmatch those required for Cyber Essentials.
Measures planned to achieve compliance / mitigate the risk with dates:	Upon selection for this contract, Acme Manufacturing will initiate an action plan to achieve Cyber Essentials Plus for the systems that manage MODII. The further controls required for the Cyber Risk Profile will also be addressed. An action plan to achieve this has been created as part of this bid and funding to achieve this plan will be made available once the contract has been awarded. No MODII will be transferred prior to the IT systems achieving the required standard. Please see separate sheet for further details.
Anticipated date of compliance / mitigations in place:	2 months after contract award.
Risk Accepted and by whom:	Yes / No
Notified (If applicable):	Yes / No
Decision recorded on Octavian:	Yes / No
Name	MOD employee
Position	MOD post
Date	MOD to complete

Example 2

Example of control-to-control commentary required to demonstrate compliance

Example at Cyber Risk Profile Moderate.

Here one control from DEFSTAN 05-138 has been selected with an example of the detail needed to evidence compliance.

DEFSTAN 05-138 control	ISO27001 control	Supplier's comment
M.01 Define and implement a policy that provides for regular, formal information security related reporting.	**Reporting information security events and weaknesses.** **Responsibilities and procedures Control Management** Responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	The ISO27001 control is enforced on the IT systems which will process MODII. A policy is in place and is enforced through management checks and regular, formal security reports are established.

Example 3

Example of control to control commentary required to demonstrate compliance

Example at Cyber Risk Profile Very Low (Cyber Essentials).

Here Cyber Essentials has been selected with examples of the detail needed to evidence compliance. Annex B from DEFSTAN 05-138 must also be completed.

Preamble

Acme manufacturing is a small company and recently invested in meeting the controls in ISO27001 as a requirement for a previous customer. Cyber Risk Management is now a board agenda item and discussed when the Board meets, which is every 3 months. The operational management level under the board is the Executive Committee which meets at least once a month and has Cyber Risk Management as a standing agenda item.

Whist Acme Manufacturing does not hold a Cyber Essentials Certificate, it does enforce the controls required through compliance with ISO27001 and the firm's governance of Cyber Risk Management. Evidence to support this application via a Cyber Implementation Plan is below.

Table Evidencing Acme Manufacturing meets the Controls required for Cyber Risk Profile Very Low

DEFSTAN 05-138 controls **Very Low** (Cyber Essentials)	**ISO27001 controls**	**Supplier's comment**
1. Boundary firewalls and internet gateways - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.	**Network controls** Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. **Security of network services** Control Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	The network upon which MODII will be processed has boundary firewalls and Internet gateways which are managed by a third party. Regular audits check the state of these devices and an annual penetration test informs the vulnerability management process. The third party supplier is responsible for software and hardware updates and these are routinely reviewed at the IT Security Working Group reporting up to the Executive Committee via the Head of IT.

DEFSTAN 05-138 controls **Very Low** (Cyber Essentials)	ISO27001 controls	Supplier's comment
2. Secure configuration – ensuring that systems are configured in the most secure way for the needs of the organisation	**Network access control** **Objective:** To prevent unauthorized access to networked services. **User authentication for external connections** Appropriate authentication methods shall be used to control access by remote users. **Equipment identification in networks** Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment. **Remote diagnostic and configuration port protection** Physical and logical access to diagnostic and configuration ports shall be controlled. **Segregation in networks** Groups of information services, users, and information systems shall be segregated on networks. **Network connection control** For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted,	The network upon which MODII will be processed is configured in such a way as to ensure easy management and oversight. The relevant controls from ISO27001 are shown on the left and these are included in the Information Security Management System which mandates routine checks of use of the network and boundary configuration. A Network Manager is employed within the IT department to ensure these controls are enforced. Furthermore, changes to the network are scheduled through the Change Advisory Board which has a security representative as a standing member.

DEFSTAN 05-138 controls Very Low (Cyber Essentials)	ISO27001 controls	Supplier's comment
	in line with the access control policy and requirements of the business applications. **Network routing control** Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. **Change control procedures** The implementation of changes shall be controlled by the use of formal change control procedures.	
3. Access control – Ensuring only those who should have access to systems to have access and at the appropriate level.	**Segregation of duties** Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisation's assets. **User access management** To ensure authorised user access and to prevent unauthorised access to information systems. **User registration** There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and	The network upon which MODII will be processed is configured in such a way as to ensure appropriate access permissions. The relevant controls from ISO27001 are shown on the left and these are included in the Information Security Management System. The HR team also informs IT Admin of new joiners, those who have left and any changes in role which may affect user access.

DEFSTAN 05-138 controls **Very Low** (Cyber Essentials)	ISO27001 controls	Supplier's comment
	services. **Privilege management** The allocation and use of privileges shall be restricted and controlled. **Review of user access rights** Management shall review users' access rights at regular intervals using a formal process. **Network access control** **Objective:** To prevent unauthorized access to networked services. **Policy on use of network services** Users shall only be provided with access to the services that they have been specifically authorized to use. **Monitoring Objective** To detect unauthorised information processing activities. **Audit logging** Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future	

DEFSTAN 05-138 controls **Very Low** (Cyber Essentials)	ISO27001 controls	Supplier's comment
	investigations and access control monitoring. **Monitoring system use** Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	
4. Malware protection – ensuring that virus and malware protection is installed and is it up to date	**Protection against malicious and mobile code** To protect the integrity of software and information. **Controls against malicious code** Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. **Security of system files** To ensure the security of system files. **Control of operational software** There shall be procedures in place to control the installation of software on operational systems.	The network upon which MODII will be processed is managed in such a way as to ensure appropriate updates are installed in a reasonable timeframe. The relevant controls from ISO27001 are shown on the left and these are included in the Information Security Management System. In addition, Acme Manufacturing utilises a third party, *PhishThem*, to conduct quarterly Phishing tests, the results of which are reported to the Executive Committee. This is evidence of Acme Manufacturing's commitment to ongoing education and employee awareness of developing threats.

DEFSTAN 05-138 controls **Very Low** (Cyber Essentials)	ISO27001 controls	Supplier's comment
5. Patch management – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.	Nil.	The network upon which MODII will be processed is managed in such a way as to ensure appropriate updates are installed in a reasonable timeframe. A software tool is employed by the IT Department to routinely scan the applications in use and to report on outdated and malicious software. An application inventory is held by the IT Department. Patch Management is a standing agenda item on the Change Advisory Board.

ACCEPTABLE CIP SUBMISSION EXAMPLE 4

Defence Standard

Defence Standard 05-138 Issue 2 states:

a. The Cyber Implementation Plan (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, and it provides an indicative template for the CIP.

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

c. The agreed plan must form part of the final contract award or amendment. The project team or buyer must periodically review the plan to ensure progress within the agreed timeframe.

d. The level of approval required for acceptance of risk on top tier contracts for High risk contracts can only be accepted by DAIS (Defence Assurance and Information Security) accreditors on behalf of the MOD SIRO.

Cyber Implementation Plan

Contract title	Special Widget 007
MOD contract number	Business Unit to complete
CSM Risk Reference	Business Unit to complete
CSM Risk Level	Business Unit to complete
Name of Supplier	ACME UK
Current level of Supplier compliance	H.08 Non-compliant. Administrative accounts (including service accounts with interactive logon) for ACME UK in-house enterprise IT systems do not use 2FA. H.10 Partially compliant.

Contract title	Special Widget 007
	ACME UK currently applies technical controls around the use of removable media, which requires all data to be encrypted where write access is permitted. Follow-your printing is enabled on printers, which ensures a user has to authenticate to print. In addition, there is a protective monitoring service managed by the Security Operations Centre and an enhanced Insider Threat monitoring capability which monitors, detects and investigates unusual / suspicious activity.
Reasons unable to achieve full compliance 1.1.1.2 1.1.1.3 1.1.1.4	H.08 ACME UK has initiated a project [OITS 1215] to implement 2FA for all administrative accounts. The Department of Defense's (DoD) DFARS regulation has made the implementation of 2FA for administrative accounts more complex than it would have been otherwise due to the requirement to provide 2FA for *all* accounts by 31 December 2017. Whilst our administrator accounts are 'first on the list' we need to consider both requirements together as it would be impractical to consider these as two separate requirements. The Company needs a coherent solution that satisfies both the MOD and DoD's requirements. The project is currently in Definition so will not have implemented 2FA by Contract Award. **H.10** Current ACME UK policy does not require certain sensitive information (such as personally identifiable information, email classifications, keywords, SSL inspection etc. and other document characteristics) to be blocked. In addition, the Company has raised concerns with the MOD about how this control can be implemented technically if there is no requirement to mark documents as MOD Identifiable Information. Until this concern has been addressed the Company cannot proceed with implementing a solution that is fully compliant.
1. Measures planned to achieve compliance / mitigate the risk with dates	**H.08** There is a funded project (Onsite IT Services' Project 1815). The project is currently nearing the end of Definition. IT Security has reviewed the number of administrative accounts and reduced these to the minimum levels needed to support the network. The list of administrative accounts is reviewed monthly central IT Security function to ensure only those with a need for an account have one, and those that no longer have a need are removed. The number of Domain Administrators has been reduced to 30 accounts. Phase 1 will deliver 2FA to these Domain Accounts as these are the high-risk accounts.

Contract title	Special Widget 007
	All requests for the issue of an administrative account are stringently reviewed and those that are approved have to go through additional security and vetting checks before an account is issued. ACME UK is also in the process of implementing an Insider Threat Programme, which is currently going through a Pilot. All administrative account holders will be required to participate in the and Privileged Vetting Procedure (PVP) – this standard will identify account holders who should not have this type of account or who may pose a threat to the Company and will have their access removed, or be denied an account. In addition, real-time monitoring on administrative accounts for anomalous activity will be taking place. **H.10** ACME UK has a funded programme (Boundary Protect) which is implementing Email and Web Guards on the boundary of the network to inspect content for sensitive information, which will block and manage content as necessary. Discussions are underway with the Boundary Protect Programme about how the capability can be leveraged to deliver H.10. Pending the outcome of our discussions with the MOD this may change our approach to meeting this requirement. Agreement has been reached on how the requirement of H.10 can be added to the existing Boundary Protect Programme. Once the MOD has responded to the Company's query the appropriate change request will be levied on the Controlled Export Compliance (International)) project. Alternatively, the capability is being deployed early to Onsite IT Services (OITS) (internal systems integrator for ACME UK) to be leveraged for the Insider Threat Programme with initial discussions having taken place on how the deployment can be used to meet the requirement of H.10.
2. Anticipated date of compliance / mitigations in place	**H.08** A confirmed date will not be known until the end of the Definition phase; however, 2FA will have been delivered for the Domain Administrators no later than 31 December 2017. **H.10** OITS deployment is expected to go-live in Q1/18, at which point the Company could be compliant. Worst case, the Web Guard is scheduled to rollout from Q2/18 at which point this control will be fully compliant. This is dependent on the ongoing discussion highlighted above. Depending on the outcome of our query with MOD, the control could be delivered earlier.
Risk Accepted and by Whom	Yes / No
Notified (If applicable)	Yes / No
Decision recorded on Octavian	Yes / No

Contract title	Special Widget 007
Name	Jules Watt
Position	Head of IT / SVP Operational Systems
Date	1 Jan 2018

Annex E

Documents Acceptable to Validate a User's Identity

The following items are acceptable to validate user identity:

- Passport
- Driving licence
- National identity card
- Proof of age card
- Adoption certificate
- Marriage certificate
- Current account
- Credit card account
- Savings account
- Mortgage account
- Loan account (excluding pay-day loans)
- Mobile phone contract
- Property rental or purchase agreement
- Buildings, contents or vehicle insurance

Annex F

Definitions and Abbreviations

Definitions

Accreditation.

Accreditation means accredited by the MOD or by an authority whose accreditation is acceptable to the MOD.

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.

Where the contract is between the MOD and the prime supplier the MOD is The Authority. Where the contract is between the prime and any sub-contractor, the prime supplier becomes The Authority.

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 authoritative definition 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

CES	Cyber Essentials Scheme	ISACA	Information Systems Audit and Control Association
CES+	Cyber Essentials Scheme Plus	JSP	Joint Services Publication
CIP	Cyber Implementation Plan	MOD	Ministry of Defence
CSM	Cyber Security Model	MODII	MOD Identifiable Information
DAIS	Defence Assurance and Information Security	PSyA	Principle Security Advisor
DCPP	Defence Cyber Protection Partnership	RA	Risk Assessment
DEFCON	Defence Condition	RAR	Risk Assessment Reference
DEFSTAN	Defence Standard	SAQ	Supplier Assurance Questionnaire
FLC	Front Line Command	SIRO	Senior Information Risk Owner
ITT	Invitation to Tender	TLB	Top Level Budget (i.e. a large organisation within the MOD)