Ministry of Defence

Industry Security Notice

Number 2017/04

Subject: **Industry Supplier Guidance on DEFCON 658 (Cyber)**

Introduction

1. The purpose of this Industry Security Notice (ISN) is to inform suppliers to the MOD on DEFCON 658 (Cyber) and its implementation using the Cyber Security Model to ensure the protection of the defence supply chain from cyber threat.

2. This ISN provides guidance to those organisations who either are suppliers to, or wish to become suppliers, to Defence on the Defence Cyber Protection Partnership (DCPP) and the Cyber Security Model (CSM). The CSM enables a risk-based approach to protect MOD Identifiable Information (MODII) as it is passed down the supply chain. Annex A provides a definition of MODII. This ISN should be read in conjunction with DEFCON 658 (Cyber) and DEFSTAN 05-138 (*see Link to DEFSTAN Web (Standardization Policy*) - http://dstan.uwh.diif.r.mil.uk). DEFSTAN 05-138 is currently under review for re-issue later this year.

3. From **October 2017** all suppliers to Defence who bid for new contracts and who process MODII will need to abide by DEFCON 658 and meet the standards mandated in DEFSTAN 05-138.

Issue

4. From 3 April 2017 DEFCON 658 was enforced for all new contracts but only to suppliers who supply direct to the MOD. The next step is for the enforcement of DEFCON 658 to flow-down the supply chain, for new contracts which handle MODII, from October 2017.

Definitions

5. The following terms are used in this notice:

MOD Identifiable Information (MODII) – MODII is defined at Annex A.

Cyber Security Model – The process by which the authority ensures its requirements to protect MODII from cyber-attack are implemented. The model has three steps: a risk assessment, a supplier assurance questionnaire and a review, by the purchasing authority, of the submitted information.

Cyber Implementation Plan – As detailed in DEFSTAN 05-138, this 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 of current level of compliance, the planned measures to achieve compliance or the proposed mitigations for consideration.

Cyber Risk Profile – This sets out the cyber protection measures required at each level of cyber risk. The required controls are detailed in DEFSTAN 05-138. If a contract is assessed as carrying a cyber risk of 'Low' then the applicant will need to comply with the measures set out in the 'Low' Profile. These requirements are progressive as one moves up the risk profiles.

Supplier Assurance Questionnaire – This is part of the Cyber Security Model and is used by the contractor to demonstrate compliance with the cyber protection requirements. All Supplier Assurance Questionnaires will be completed using the online tool.

Cyber Essentials – This scheme, managed by the National Cyber Security Centre, defines a set of controls which, when properly implemented will provide organisations with basic protection from the most prevalent forms of threat.

Background

6. The DCPP is a joint MOD and industry initiative established to improve the protection of the defence supply chain from cyber threats. A CSM has been established by the DCPP, and the MOD will initiate it for each contract with the aim of protecting MODII. The buyer within the MOD will go through the risk assessment process, which will create a Cyber Risk Profile and subsequently mandate appropriate cyber controls for suppliers.

7. From 3 April 2017 DEFCON 658 was enforced for all new contracts but only to suppliers who supply direct to the MOD. The next step is for enforcement of the DEFCON to flow-down the supply chain, for new contracts only, from October 2017.

8. The three components of the CSM are detailed below:

- The Risk Assessment (RA), this is conducted to evaluate the degree of cyber risk to a specific contract which contains MODII, and establishes a Cyber Risk Profile;

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

- An evaluation of the SAQ and any supporting evidence, such as a CIP, by the buyer which will form a factor in considering if a contract should be awarded.

Process

9. The process the MOD uses to guarantee its information has sufficient protection from a cyber threat is the CSM. More detail on this three stage process is below:

10. For all new requirements, it is mandatory a RA is completed using the online tool. Once completed, one of five Cyber Risk Profiles will be arrived at. A Cyber Risk Profile details a series of controls deemed necessary for a supplier to hold MODII, dependent upon the output of the RA. Suppliers can currently access the online tool at https://suppliercyberprotection.service.xgov.uk/ .

11. Upon completion of a RA, a unique Risk Assessment Reference (RAR) will be awarded.

12. The RAR will be used by potential future suppliers allowing them to react to the ITT and complete an SAQ in response.

13. It is essential the SAQ is filled out by buyers who are bidding for a contract using the online tool. Suppliers must input the RAR of the contract and will be required to answer specific questions which relate to the level of cyber risk for that contract.

14. If a supplier fails to fulfil the conditions of the cyber risk profile, they have an option to commit to obtain compliance before or at the start date of contract award using a CIP. The CIP, which is detailed in DEFSTAN 05-138, will provide evidence as to how suppliers will achieve compliance, and when they will achieve it.

15**. From October 2017 DEFCON 658 will apply to all suppliers** down the supply chain, where MODII flows-down and therefore a RA will be completed by suppliers for sub-contracts, for suppliers who wish to bid for a contract. A newly generated RAR will then be distributed to potential sub-contractors and this will generate further SAQs which may be considered prior to contract award. This process proceeds down the supply chain up to a point where MODII is neither moved, saved nor electronically retrieved.

Cyber Risk Profiles

16. Below is a list of the cyber risk profiles and the corresponding controls. Detail on the controls are set out in DEFSTAN 05-138:

- N/A- No action required. Although the DCPP advises all suppliers to achieve Cyber Essentials as a minimum.
- Very Low - Cyber Essentials certification.
- Low - Cyber Essentials Plus certification.
- Moderate - All the requirements of ‘Low’ and additional controls.
- High – All the requirements of ‘Moderate’ and additional controls.

Cyber Essentials Certification

17. The lowest necessity of a contract where the transfer, storage or access of MODII takes place electronically is a Cyber Essentials certificate. Cyber Essentials is a standard established by the National Cyber Security Centre to provide protection from the most basic, yet common threats.

Action by Industry

18. To follow the guidance of this ISN and follow the procedures defined by DEFCON 658 and DEFSTAN 05-138. In engaging with these policies Industry is ensuring they are following the Cyber Security Model, in which suppliers confirm they maintain the requisite cyber security controls and they are in place before contract award. This action supports the UK's National Cyber Security Strategy and National Security Strategy.

Validity / Expiry Date

19. This notice is valid with immediate effect and remains so until further notice.

MOD Point of Contact Details

20. Ministry of Defence, Main Building, Cyber Industry Team, DAIS, Whitehall, Westminster, London SW1A 2HB.

Telephone: 0207 218 3650 Email: ISSDes-DCPP@mod.uk

Annex A Definition of MOD Identifiable Information

Annex A

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.

1. Definitions

1.1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

"**Associated Company**" means:

(a) any associated company of the Contractor from time to time within the meaning of Section 449 of the Corporate Tax Act 2010 or any subordinate legislation; and

(b) any parent undertaking or subsidiary undertaking of the Contractor from time to time within the meaning of section 1162 Companies Act 2006 and it is further agreed that where the ownership of shares in any such undertaking have been pledged or transferred to a third party by way of security, the original parent shall still be considered a member of the subsidiary undertaking;

"**Contractor Deliverables**" shall have the meaning set out in DEFCON 501;

"**Cyber Risk Level**" means the level of Cyber Risk relating to this Contract assessed in accordance with the Cyber Security Model;

"**Cyber Security Implementation Plan**" means the plan referred to in Clause 3 of this Condition including but not limited to any risk-balance case and mitigation measures required by the Authority;

"**Cyber Security Incident**" means an event, act or omission which gives rise or may give rise to:

(a) unauthorized access to an information system or electronic communications network;

(b) disruption or change of the operation (including but not limited to takeover of control) of an information system or electronic communications network;

(c) destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network;

(d) removal or limiting the possibility to use MOD Identifiable Information residing in an information system or electronic communications network; or

(e) the appropriation, publication, dissemination or any other use of non-public MOD Identifiable Information by persons unauthorised to do so.

"**Cyber Security Instructions**" means DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Contract issued by the Authority to the Contractor;

"**Cyber Security Model**" and "CSM" mean the process by which the Authority ensures that MOD Identifiable Information is adequately protected from Cyber Incident and includes the CSM Risk Assessment Process, DEFSTAN 05-138 and the CSM Supplier Assurance Questionnaire;

"**CSM Risk Assessment Process**" means the risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Level for this Contract and any Sub-contract;

"**CSM Supplier Assurance Questionnaire**" means the supplier assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Contractor to demonstrate compliance with this Condition;

"**Data**" means any data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media.

"**DEFSTAN 05-138**" means the Defence Standard 05-138 as amended or replaced from time to time;

"**Electronic Information**" means all information generated, processed, transferred or otherwise dealt with under or in connection with the Contract, including but not limited to Data, recorded or preserved on any information system or electronic communications network;

"**Good Industry Practice**" means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgment and the making of any expenditure that would reasonably be expected from a skilled person in the same type of undertaking under the same or similar circumstances;

"**ISN**" means Industry Security Notices issued by the Authority to the Contractor whether directly or by issue on the gov.uk website at: https://www.gov.uk/government/publications/industry-security-notices-isns;

"**JSyCC WARP**" means the Joint Security Co-ordination Centre MOD Defence Industry Warning, Advice and Reporting Point or any successor body notified by way of ISN;

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

"**NSA/DSA**" means, as appropriate, the National or Designated Security Authority of the Contractor that is responsible for the oversight of the security requirements to be applied by the Contractor and for ensuring compliance with applicable national security regulations;

"**Sites**" means any premises from which Contractor Deliverables are provided in connection with this Contract or from which the Contractor or any relevant Sub-contractor manages, organises or otherwise directs the provision or the use of the Contractor Deliverables and/or any sites from which the Contractor

or any relevant Sub-contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Contract;

"**Sub-contractor**" means a sub-contractor of the Contractor or any Associated Company whether a direct Sub-contractor or at any lower level of the supply chain who provides any Contractor Deliverables in connection with this Contract;

"**Supplier Cyber Protection Service**" means the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire.

2. Authority Obligations

2.1. The Authority shall:

2.1.1. determine the Cyber Risk Level appropriate to this Contract and, where the Contractor has not already been notified of the Cyber Risk level prior to the date of this Contract, shall provide notification of the relevant Cyber Risk level and the appropriate Cyber Security Instructions to the Contractor as soon as is reasonably practicable; and

2.1.2. notify the Contractor as soon as reasonably practicable where the Authority reassesses the Cyber Risk Level relating to this Contract .

3. Contractor Obligations

3.1. The Contractor shall:

3.1.1. comply with DEFSTAN 05-138;

3.1.2. complete the CSM Risk Assessment Process in accordance with the Authority's instructions and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Contractor's supply chain which has or may have an impact on the Cyber Risk Level of this Contract or on receipt of any reasonable request by the Authority;

3.1.3. carry out the CSM Supplier Assurance Questionnaire no less than once in each year of this Contract commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire;

3.1.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge its obligations under this Condition in accordance with Good Industry Practice *provided always that* where there is a conflict between the Contractor's obligations under 3.1.1 above and this 3.1.4 the Contractor shall notify the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as it becomes aware of the conflict and the Authority shall determine which standard or measure shall take precedence;

3.1.5. comply with all Cyber Security Instructions notified to it by the Authority as soon as reasonably practicable;

3.1.6. notify the JSyCC WARP in accordance with ISN 2014/02 as amended or updated from time to time and the Contractors NSA/DSA immediately in writing as soon as they know or believe that a Cyber Security Incident has or may have taken place providing full details of the circumstances of the incident and any mitigation measures already taken or intended to be taken;

3.1.7. in coordination with its NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the Authority and its agents and representatives and its NSA/DSA to take all steps to mitigate the impact of the Cyber Security Incident and minimise the likelihood of any further similar Cyber Security Incidents. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the Contractors NSA/DSA in the circumstances and taking into account the Cyber Risk Level; and

3.1.8. consent to the Authority recording and using information obtained in relation to the Contract for the purposes of the Cyber Security Model whether on the Supplier Cyber Protection Service or elsewhere. For the avoidance of doubt such information shall include the cyber security accreditation of the Contractor

PROVIDED ALWAYS THAT where the Contractor has notified the Authority that it cannot comply with 3.1.1 to 3.1.8 above the Authority and Contractor will seek to agree a Cyber Security Implementation Plan and where the Authority has agreed a Cyber Security Implementation Plan with the Contractor, the Contractor shall comply with such Cyber Security Implementation Plan until implementation is agreed to have been achieved whereupon 3.1.1 to 3.1.9 above shall apply in full. In the event that a Cyber Security Implementation Plan cannot be agreed the provisions of DEFCON 530 or any agreed alternative dispute resolution procedure shall apply.

4. Records

4.1. The Contractor shall keep and maintain until 6 years after termination or expiry of this Contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:

4.1.1. details of all MOD Identifiable Information relating to the Contractor Deliverables provided under this Contract; and

4.1.2. copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor.

4.2. The Contractor shall on request provide the Authority, the Authority's representatives and/or the Contractors NSA/DSA such access to those records as may be required in connection with this Contract.

5. Audit

5.1. Except where an audit is imposed on the Authority by a regulatory body or there is a Cyber Security Incident in which case the Contractor agrees that the Authority and its representatives, in coordination with the Contractors NSA/DSA or the NSA/DSA on behalf of the Authority, may conduct such audits as it considers in its absolute opinion necessary, the Authority, its representatives and/or the Contractors NSA/DSA may, not more than twice in any calendar year and for a period of 6 years following the termination or expiry of this Contract, whichever is the later, conduct an audit for the following purposes:

5.1.1. to review and verify the integrity, confidentiality and security of any MOD Identifiable Information;

5.1.2. to review the Contractor's compliance with its obligations under this Condition; and

5.1.3. to review any records created during the provision of the Contractor Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of 5.1.1 and 5.1.2 above.

5.2. The Authority shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor or delay the provision of the Contractor Deliverables and supplier information received by the Authority in connection with the audit shall be treated as confidential information.

5.3. The Contractor shall on demand provide the Authority and any relevant regulatory body, including the Contractor's NSA/DSA, (and/or their agents or representatives), together "the Auditors", with all reasonable co-operation and assistance in relation to each audit, including but not limited to:

5.3.1. all information requested by the Authority within the permitted scope of the audit;

5.3.2. reasonable access to any Sites controlled by the Contractor or any Associated Company and any Sub-contractor and to any equipment used (whether exclusively or non-exclusively) in the performance of the Contract and, where such Sites and/or equipment are outwith the control of the Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

5.3.3. access to any relevant staff.

5.4. The Authority shall endeavour to (but is not obliged to) provide at least 15 calendar days notice of its intention to conduct an audit.

5.5. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Condition, unless the audit identifies a material breach of the terms of this Condition by the Contractor in which case the Contractor shall reimburse the

Authority for all the Authority's reasonable costs incurred in the course of the audit.

6. Breach of Obligations

6.1. In exercising its rights or remedies under this Condition, the Authority shall:

6.1.1. act in a reasonable and proportionate manner having regard to such matters as the gravity of any breach or potential breach and the Cyber Risk Level of this Contract; and

6.1.2 give all due consideration, where appropriate, to action other than termination of the Contract, including but not limited to a remedial period if this is appropriate in all the circumstances.

6.2. Where the Cyber Risk Level of this Contract is assessed to be a **moderate or high**, and the Contractor breaches the terms of this Condition, the Authority shall be entitled:

6.2.1 to terminate the Contract (whether in whole or in part) and to claim damages in accordance with DEFCON 514 as though such breach is a material breach; and

6.2.2 where the Contract has not been terminated, to recover from the Contractor any other loss sustained in consequence of any breach of this Condition, subject to any provision which is agreed elsewhere in this Contract.

6.3. Where the Cyber Risk Level of this Contract is assessed to be **very low or low**, and the Contractor breaches the terms of this Condition, the Authority shall be entitled:

6.3.1. to recover from the Contractor the amount of any loss sustained in consequence of any breach of this Condition, subject to any provision which is agreed elsewhere in this Contract; and

6.3.2. where the Contractor does not comply with any reasonable instructions issued by the Authority or the Contractors NSA/DSA within the time period specified to remedy such breach or prevent further breaches, the Authority shall be entitled to terminate this Contract (whether in whole or in part) and to claim damages in accordance with DEFCON 514 as though such breach is a material breach.

6.4 Where the Contractor commits an act of fraud, negligence or wilful misconduct in respect of its obligations under this Condition the Authority shall be entitled to terminate this Contract (whether in whole or in part) and to claim damages in accordance with DEFCON 514 as though such breach is a material breach.

7. General

7.1. On termination or expiry of this Contract the provisions of this Condition excepting 3.1.2 and 3.1.3 above shall continue in force so long as the Contractor holds any MOD Identifiable Information relating to this Contract.

7.2. Termination or expiry of this Contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination or expiry.

7.3.

7.3.1. The Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 and/or the Cyber Risk Level. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Level, then either Party may seek an adjustment to the Contract Price for any associated increase or decrease in costs and the Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Level *provided always that* the Contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and *further provided that* such costs shall not be allowed unless they are considered to be appropriate, attributable to the Contract and reasonable in all the circumstances.

7.3.2. Subject to 7.3.1 above, where the Contractor seeks such adjustment or extension, the Authority will proceed in accordance with DEFCON 620 or any agreed alternative change control procedure to determine the request for adjustment or extension. The Contractor must deliver a Contractor Change Proposal to the Authority within 8 weeks of the occurrence of the change in DEFSTAN 05-138 or Cyber Risk Level or such longer period as may be agreed by the Parties, identifying the impact of that change and accompanied by full details of the request for adjustment. For the avoidance of doubt, the Authority shall not be required to withdraw any Authority Notice of Change which may have been issued insofar as it relates to DEFSTAN 05-138 or the Cyber Risk Level whether or not the Contractor Change Proposal is rejected. In the event that the Contractor does not agree with the Authority's determination, then the provisions of DEFCON 530 or any agreed alternative dispute resolution procedure shall apply.

7.4. The Contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other losses are recoverable or have been recovered by the Contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Cyber Security Incident or otherwise, where the Contractor is able to or has recovered such sums in any other provision of this Contract or has recovered such costs and/or losses in other contracts between the Contractor and the Authority or with other bodies.