SCHEDULE 32

Cyber Provisions to be Included in Relevant Sub-Contracts

1 DEFINITIONS

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

Authority	the Secretary of State for Defence at Ministry of Defence, Whitehall, London SW1A 2HB;
Associated Company	(a) any associated company of the Sub-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 Sub-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;
CSM Risk Assessment Process	the risk assessment process which forms part of the Cyber Security Model and is used to measure the Cyber Risk Profile for this Sub-Contract and any lower tier Sub-Contract;
CSM Contractor Assurance Questionnaire	the Contractor assessment questionnaire which forms part of the Cyber Security Model and is to be used by the Sub-Contractor to demonstrate compliance with this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts);
Cyber Implementation Plan	the plan referred to in Paragraph 2.1 (a) of this Schedule;
Cyber Risk Profile	the level of cyber risk relating to this Sub-Contract or any lower tier Sub-Contract as assessed in accordance with the Cyber Security Model;
Cyber Security Incident	an event, act or omission which gives rise or may give rise to: (a) unauthorised access to an information system or electronic communications network on which MOD Identifiable Information resides; (b) disruption or change of the operation (including but not limited to takeover of control) of an information system or

	electronic communications network on which MOD Identifiable Information resides; (c) unauthorised destruction, damage, deletion or the change of MOD Identifiable Information residing in an information system or electronic communications network; (d) unauthorised or unintentional 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	DEFSTAN 05-138, together with any relevant ISN and specific security instructions relating to this Sub-Contract issued by the Authority to the Prime Contractor;
Cyber Security Model or "CSM"	mean the process by which the Authority ensures that MOD Identifiable Information is adequately protected from Cyber Security Incident and includes the CSM Risk Assessment Process, DEFSTAN 05-138 and the CSM Contractor Assurance Questionnaire conducted via the Contractor Cyber Protection Service;
Data	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	the Defence Standard 05-138 as amended or replaced from time to time;
Electronic Information	all information generated, processed, transferred or otherwise dealt with under or in connection with this Sub-Contract, including but not limited to Data, recorded or preserved in electronic form and held on any information system or electronic communications network;
Good Industry Practice	the exercise of that degree of skill, care, prudence and foresight and operating practice which would reasonably and ordinarily be expected from time to time of a skilled and experienced operator seeking in good faith to comply with all its contractual obligations and all applicable Law and engaged

	in the same type of undertaking under the same or similar circumstances;
ISN	Industry Security Notices issued by the Authority to the Prime Contractor whether directly or by issue on the gov.uk website at: https://www.gov.uk/government/publications/industry-security-notices-isns;
JSyCC WARP	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	all Electronic Information which is attributed to or could identify an existing or proposed Authority capability, defence activities or personnel and which the Authority requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure;
NSA/DSA	as appropriate, the National or Designated Security Authority of the Prime Contractor or Sub-Contractor that is responsible for the oversight of the security requirements to be applied by the Prime Contractor or Sub-Contractor and for ensuring compliance with applicable national security regulations;
Prime Contract	the Contract titled ("Contract 4 (Off-shore Support to Military Training and Exercises)") made between the Authority and the Contractor;
Prime Contractor	the Contractor named in the Prime Contract with the Authority;
Sites	any premises from which Services are provided in connection with this Sub-Contract or from which the Sub-Contractor or any relevant lower tier Sub-Contractor manages, organises or otherwise directs the provision or the use of the Services and/or any sites from which the Sub-Contractor or any relevant lower tier Sub-Contractor generates, processes, stores or transmits MOD Identifiable Information in relation to this Sub-Contract;
Sub-Contract	any sub-contract at any level of the supply chain, whether this Sub-Contract which is awarded by the Prime Contractor or any related Sub-Contract which is awarded by the Sub-Contractor or any lower tier Sub-Contractor or Associated Company, which is entered into as a consequence of or in connection with this Sub-Contract;
Sub-Contractor	a Sub-Contractor of the Prime Contractor or any Associated Company whether a direct Sub-Contractor or at any lower level of the supply chain who provides any Services in connection

	with the Prime Contract but only to the extent that the Sub-Contractor processes, stores or transmits MOD Identifiable Information under their Sub-Contract;
Contractor Cyber Protection Service	the tool incorporating the CSM Risk Assessment Process and CSM Contractor Assurance Questionnaire.

2 SUB-CONTRACTOR OBLIGATIONS

2.1 The Sub-Contractor shall, and shall procure that their lower tier Sub-Contractors shall:

(a) comply with DEFSTAN 05-138 or, where applicable, the Cyber Implementation Plan attached to this Sub-Contract and for the avoidance of doubt any Cyber Implementation Plan shall be prepared and implemented in accordance with Good Industry Practice taking account of any risk-balance case and any mitigation measures required by the Authority and the Prime Contractor and shall ensure that any measures taken to protect MOD Identifiable Information are no less stringent than those taken to protect their own proprietary information;

(b) complete the CSM Risk Assessment Process in accordance with the Authority and the Prime Contractor's instructions, ensuring that any change in the Cyber Risk Profile is notified to the Authority, the Prime Contractor and any affected lower tier Sub-Contractor, and complete a further CSM Risk Assessment Process or CSM Contractor Assurance Questionnaire where a change is proposed to the supply chain or on receipt of any reasonable request by the Authority;

(c) re-perform the CSM Contractor Assurance Questionnaire no less than once in each year of this Sub-Contract commencing on the first anniversary of completion of the CSM Contractor Assurance Questionnaire to demonstrate continued compliance with the Cyber Security Instructions;

(d) having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge their obligations under this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) in accordance with Good Industry Practice provided always that where there is a conflict between the Sub-Contractor's obligations under 2.1(a) above and this 2.1(d) the Sub-Contractor shall notify the Prime Contractor and the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as they become aware of the conflict and the Authority shall determine which standard or measure shall take precedence;

(e) comply with all Cyber Security Instructions notified to them by the Authority and/or the Prime Contractor as soon as reasonably practicable;

(f) notify the JSyCC WARP in accordance with ISN 2017/03 as amended or updated from time to time and the Prime Contractor and the Sub-Contractor's NSA/DSA immediately in writing as soon as they know or believe that a Cyber Security Incident has or may

have taken place providing initial details of the circumstances of the incident and any mitigation measures already taken or intended to be taken, and providing further information in phases, as full details become available;

(g) in coordination with their NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the Authority, the Prime Contractor and their agents and representatives 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 Authority and the relevant Prime Contractor and/or Sub-Contractor's NSA/DSA in the circumstances and taking into account the Cyber Risk Profile; and

(h) consent to the Authority recording and using information obtained via the Contractor Cyber Protection Service in relation to the Sub-Contract for the purposes of the Cyber Security Model which shall include any agreed Cyber Implementation Plan. For the avoidance of doubt such information shall include the cyber security accreditation of the Sub-Contractor and/or lower tier Sub-Contractor as appropriate; and

(i) include provisions equivalent to this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) in all lower tier Sub-Contracts (the "**equivalent provisions**") and, where a lower tier Sub-Contractor breaches terms implementing this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) in a Sub-Contract, the Sub-Contractor shall, and shall procure that their lower tier Sub-Contractors shall, in exercising their rights or remedies under the relevant Sub-Contract:

(i) notify the Prime Contractor and the Authority of any such breach and consult with the Prime Contractor and the Authority regarding any remedial or other measures which are proposed as a consequence of such breach, taking the Authority's views into consideration; and

(ii) have regard to the equivalent provisions.

3 RECORDS

3.1 The Sub-Contractor shall keep and maintain, and shall ensure that any lower tier Sub-Contractor shall keep and maintain, until six years after termination of Contract term or final payment under this Sub-Contract, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:

(a) copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts), including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Contractor Assurance Questionnaire, together with any certificates issued to the Sub-Contractor and/or any lower tier Sub-Contractor; and

(b) copies of all documents demonstrating compliance with 2.1(e) and in relation to any notifications made under 2.1(f) and/or investigation under 2.1(g).

3.2 The Sub-Contractor shall, and shall ensure that any lower tier Sub-Contractor shall, on request provide the Authority, the Authority's representatives and/or the relevant Prime Contractor or Sub-Contractor's NSA/DSA such access to those records under 3.1 as may be required in connection with this Sub-Contract.

4 AUDIT

4.1 In the event of a Cyber Security Incident the Sub-Contractor agrees that the Authority and its representatives, in coordination with the relevant Prime Contractor or Sub-Contractor's NSA/DSA, may conduct such audits as are required to establish (i) the cause of the Cyber Security Incident, (ii) the impact of the Cyber Security Incident, (iii) the MOD Identifiable Information affected, and (iv) the work carried out by the Sub-Contractor to resolve the Cyber Security Incident and to mitigate the effects, to ensure that the Cyber Security Incident is resolved to the satisfaction of the Authority and the NSA/DSA.

4.2 In addition to the rights in 4.1 above, the Sub-Contractor agrees that the Authority, its representatives and/or the relevant Prime Contractor or Sub-Contractor's NSA/DSA, either solely or in any combination, may at any time during the Contract and for a period of six years after termination of this Sub-Contract or the end of the Sub-Contract term or final payment under the Sub-Contract whichever is the later, but not more than once in any calendar year, conduct an audit for the following purposes where the Sub-Contractor continues to hold MOD Identifiable Information:

(a) to review and verify the integrity, confidentiality and security of any MOD Identifiable Information;

(b) to review the Sub-Contractor's and/or any lower tier Sub-Contractor's compliance with their obligations under DEFSTAN 05-138 or a Cyber Implementation Plan; and

(c) to review any records created during the provision of the Services, including but not limited to any documents, reports and minutes which refer or relate to the Services for the purposes of 3.1(a) and 3.1(b) above.

4.3 The Authority, acting reasonably and having regard to the confidentiality and security obligations owed by the Sub-Contractor to third parties, shall propose the scope of each audit in writing with a view to seeking the agreement of the Sub-Contractor but shall make the ultimate decision on the scope. For the avoidance of doubt the scope of the audit shall not grant the Authority any unsupervised access to any of the Sub-Contractor's information systems or electronic communications networks. The Authority and the Prime Contractor shall use their reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Sub-Contractor and/or lower tier Sub-Contractor or delay the provision of the Services and Contractor information received in connection with the audit shall be treated as confidential information.

4.4 The Sub-Contractor shall, and shall ensure that any lower tier Sub-Contractor shall, on demand provide the Authority and any relevant regulatory body, including the relevant Prime Contractor or Sub-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:

(a) all information requested by the Authority within the permitted scope of the audit;

(b) reasonable access to any Sites controlled by the Sub-Contractor or any Associated Company and any lower tier Sub-Contractor used in the performance of the Sub-Contract to the extent required within the permitted scope of the audit and, where such Sites are outwith the control of the Sub-Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

(c) access to any relevant staff.

4.5 Where the Prime Contractor is provided with notice of the audit by the Authority and/or the relevant NSA/DSA, the Prime Contractor shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice to the Sub-Contractor of the intention to conduct an audit.

4.6 The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts), unless the audit identifies a material breach of the terms of this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) by the Sub-Contractor and/or a lower tier Sub-Contractor in which case the Sub-Contractor shall reimburse the Prime Contractor and the Authority as appropriate for all the reasonable costs incurred in the course of the audit.

4.7 The Sub-Contractor shall in their lower tier Sub-Contracts procure rights for the Authority to enforce the terms of this Paragraph 4 of this Schedule in accordance with the Contracts (Rights of Third Parties) Act 1999.

5 GENERAL

5.1 On termination or expiry of this Sub-Contract the provisions of this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) shall continue in force so long as the Sub-Contractor and/or any lower tier Sub-Contractor holds any MOD Identifiable Information relating to this Sub-Contract.

5.2 Termination or expiry of this Sub-Contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) 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 this Sub-Contract which existed at or before the date of termination or expiry.

5.3 The Sub-Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 or the Cyber Risk Profile or both and issue new or updated Cyber Security Instructions. In the event that there is such a change to DEFSTAN 05-138 or the Cyber Risk Profile or both, then the Sub-Contractor may seek an adjustment to the contract price from the Prime Contractor for any associated increase or decrease in costs and the Sub-Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Profile or both provided always that the Sub-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 this Sub-Contract and reasonable in all the circumstances.

5.4 The Sub-Contractor shall not recover any costs and/or other losses under or in connection with this Schedule 32 (Cyber Provisions to be Included in Relevant Sub-Contracts) where such costs and/or other losses are recoverable or have been recovered by the Sub-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 Sub-Contractor is able to or has recovered such sums in any other provision of this Sub-Contract or has recovered such costs and/or losses in other contracts between the Sub-Contractor and the Prime Contractor or with other bodies.