DEFENCE AS A PLATFORM
SIP FINAL SCHEDULE 6
SECURITY REQUIREMENTS

TABLE OF CONTENTS

SCHEDULE 6

SECURITY REQUIREMENTS

Capitalised terms used but not defined in this Schedule are defined in Clause 1.1 (*Definitions and Interpretation*).

PART A

INTRODUCTION

1. INTRODUCTION

1.1 This Schedule sets out:

1.1.1 the overarching security requirements that support the delivery of the Services; and;

1.1.2 the additional cyber security requirements.

1.2 In this Schedule, the definitions set out in the table in this Paragraph 1.2 shall apply.

"**Classified Information**"	means any piece of information created, stored or processed by the Authority that is deemed to be classified by the Authority under its classification scheme;
"**CSM Risk Assessment Process**"	means the DCPP-mandated risk assessment process which forms part of the Cyber Security Model;
"**CSM Subcontractor**"	has the meaning given to it at Paragraph 6.5 of Schedule 6 (*SECURITY REQUIREMENTS*;
"**CSM Supplier Assurance Questionnaire**"	means the supplier assessment questionnaire, which forms part of the DCPP Cyber Security Model, that suppliers must complete and submit to demonstrate their ability to comply with the requirements for the Cyber Risk Level of this Agreement;
"**Cyber Incident**"	means an event, act or omission which gives rise or may give rise to: (a) unauthorised 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 Risk Level"	means the level of cyber risk relating to this Agreement or any subcontract, as applicable, assessed in accordance with the Cyber Security Model;
"Cyber Security Implementation Plan"	means the plan referred to in Paragraph 6.11 of Schedule 6 (*Security Requirements*) which shall include, but shall not be limited to, any risk-balance case and/or mitigation measures required by the Authority;
"Cyber Security Model" or **"CSM"**	mean the process by which the Authority ensures that MOD Identifiable Information is adequately protected from Cyber Incidents;
"DCPP"	means the Defence Cyber Protection Partnership, a government industry initiative to improve the protection of the defence supply chain from the cyber threat;
"DCPP Subcontractor"	has the meaning given to it at Paragraph 6.8 of Schedule 6 (*Security Requirements*);
"DEFSTAN 05-138"	means the Authority Standard identified as such in Schedule 5 (*Authority Standards*);
"HMG Personnel Security Controls"	means the HMG personnel security controls document issued by the Cabinet Office, and as amended from time to time;
"Information Assurance"	means the steps taken to verify that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users;
"Information Security Management System"	means an information security management system, designed, implemented and maintained in accordance with the latest version of ISO/IEC 27001 or equivalent standard and Schedule 6 (*Security Requirements*);
"ISN 2014/02"	means the Authority Standard identified as such in Schedule 5 (*Authority Standards*);
"ISN 2017/01"	means the Authority Standard identified as such in Schedule 5 (*Authority Standards*);
"JSyCC WARP"	means the Joint Security Co-ordination Centre Warning and Reporting Points;

"Junior CSM Subcontractor"	has the meaning given to it at Paragraph 6.7 of Schedule 6 (*Security Requirements*);
"MOD Identifiable Information"	means all electronic information generated, transferred or otherwise handled by the Contractor in connection with this Agreement which is attributed to or could identify an existing or proposed Authority capability, defence activity or personnel, and which the Authority requires to be protected against loss, misuse, alteration or unauthorised disclosure;
"Other Incident"	has the meaning given to it at Paragraph 8.1.2 of Schedule 6 (*Security Requirements*);
"Security Policy Framework"	means the security policy framework containing the primary internal protective security policy and guidance on security and risk management for Government departments and associated bodies, which: (a) is the source on which all localised security policies should be based; (b) sets out the minimum security requirements which are mandatory for all Government Departments and Agencies; and (c) also provides technical information, advice and guidance to support implementation of the policy requirements;
"Senior CSM Subcontractor"	has the meaning given to it at Paragraph 6.7 of Schedule 6 (*Security Requirements*);
"Supplier Cyber Protection Service"	means the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire; and
"Threat to Security"	means the range of security threats that is comprised of: (a) the extant traditional threat from state on state conflicts; (b) terrorism carried out by international and domestic terrorist groups; (c) espionage, including as a result of a number of foreign states seeking to acquire sensitive UK information and technologies; (d) cyber threats used by hostile actors to conduct espionage operations or launch damaging computer network attacks; and (e) asymmetric threats from non-state and failed state actors using a blend of

	tactics such as economic, cyber and proxy threat actors.

PART B

OVERARCHING SECURITY REQUIREMENTS

The overarching security requirements are intended to protect Authority assets, facilities, systems, networks, information and processes that support national security.

2. SECURITY MEASURES

2.1 Unless the Contractor has received written permission of the Authority, the Contractor shall not, and shall procure that the Contractor Personnel shall not, disclose Authority Data or allow Authority Data to be disclosed to any person:

2.1.1 who does not possess the appropriate security clearance in accordance with the Security Aspects Letter;

2.1.2 who has not been given the prior written approval by the Authority to access the Authority Data;

2.1.3 where the Authority has notified the Contractor that the Authority Data shall not be disclosed to or acquired by that person;

2.1.4 who is not a member of the Contractor Personnel; or

2.1.5 where this is not required for the proper performance of the Contract.

2.2 Unless the Contractor has received written permission of the Authority, the Contractor shall, and shall procure that the Contractor Personnel shall, take all reasonable steps to ensure that:

2.2.1 no photograph of, or pertaining to, any Authority Data shall be taken except to the extent necessary for the proper performance of this Agreement;

2.2.2 no copy of or extract from any Authority Data shall be made except to the extent necessary for the proper performance of this Agreement;

2.2.3 Authority Data is at all times strictly safeguarded in accordance with the Security Policy Framework and upon request by the Authority, is delivered up to the Authority within a reasonable period; and

2.2.4 no Authority Data is removed from any Authority Premises without written approval from the Authority.

Observation Of Regulations

2.3 The Contractor shall comply and shall ensure that Contractor Personnel and its Approved Subcontractors comply with the Authority's security policies, processes and procedures as included in the Authority Standards, and any other rules, regulations and security requirements that are in force at any Authority Premises (which shall be provided to Contractor by the Authority on request).

Development of the Information Security Management System

2.4 The Contractor shall provide documented evidence of the Contractor's Information Assurance processes, including an Information Security Management System ("**ISMS**").

2.5 The Contractor shall maintain, continuously improve and comply with, and ensure that all Contractor Personnel and Approved Subcontractors comply with, the ISMS throughout the Term (and during any Exit Period).

2.6 The Contractor shall ensure that the ISMS is at all times in accordance with the Authority Standards.

Accreditation of ICT

2.7 If the Contractor uses its ICT system for delivery of the Services, the Contractor shall take all reasonable steps to gain accreditation of its ICT system by DAIS MOD in accordance with ISN 2017/01.

Authority Requests

2.8 On receipt of a written request by the Authority, the Contractor shall promptly provide to the Authority:

2.8.1 details of Contractor Personnel who have had access to Authority Data;

2.8.2 such information as the Authority may reasonably request from time to time to demonstrate that the Contractor and the Contractor Personnel are complying with their obligations under this Schedule; and

2.8.3 full particulars of any failure by the Contractor and/or the Contractor Personnel to comply with any obligations relating to this Schedule.

2.9 If the Contractor or any of the Contractor Personnel is aware or suspects that in its reasonable opinion an unauthorised person is seeking or has sought to obtain information concerning Authority Data, the Contractor shall immediately inform the Authority in writing of this event.

3. LEVEL OF SECURITY

3.1 The Contractor shall at all times ensure that the level of security that it employs in the provision of the Services is appropriate, including in relation to the following risks:

3.1.1 loss of integrity and confidentiality of Authority Data, including Classified Information;

3.1.2 unauthorised access to, use or disclosure of, or interference with Authority Data, including Classified Information, by any person or organisation;

3.1.3 unauthorised access to network elements, buildings, the Authority Premises and tools (including equipment) used by the Contractor and any Approved Subcontractors in the provision of the Services;

3.1.4 use of the Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

3.1.5 loss of availability of Authority Data, including Classified Information, due to any failure or compromise of the Services.

3.2 The Contractor shall ensure that all Contractor Personnel:

3.2.1 receive training in the Threat to Security, as well as specific security training relevant to their role and operations requirements for the Authority Premises on which such Contractor Personnel will be located; and

3.2.2 have security clearance appropriate for the relevant Authority Premises and level of access required in accordance with HMG Personnel Security Controls as issued by the Cabinet Office and the Security Aspects Letter.

3.3 The Contractor shall:

3.3.1 record and maintain a record of security clearances of each of the Contractor Personnel;

3.3.2 provide the Authority with a copy of such a record within five (5) Working Days of the Service Commencement Date; and

3.3.3 provide the Authority with an updated record promptly following any changes to such a record.

4. BREACH OF SECURITY

4.1 Either Party shall notify the other in writing immediately upon becoming aware of any Breach of Security including an actual, potential or attempted Breach of Security, or Threat to Security.

4.2 The Contractor shall provide to the Authority full details using such reasonable reporting mechanisms as may be specified by the Authority from time to time of the Breach of

Security or the potential or attempted Breach of Security and of the steps taken to mitigate or resolve them.

4.3 The Contractor shall ensure that all Contractor Personnel are aware that personal electronic devices with a recording, photographic or transmitting capability are not allowed within certain locations that the Authority notifies to the Contractor from time to time and the Contractor shall ensure that all Contractor Personnel comply with such restrictions.

PART C

CYBER SECURITY REQUIREMENTS

The cyber security requirements provide the Authority with additional protection from cyber security risks, in addition to the overarching security requirements.

5. CONTRACTOR OBLIGATIONS

5.1 The Contractor shall implement and maintain all appropriate technical and organisational security measures in accordance with Good Industry Practice to discharge its obligations under this Part C (*CYBER SECURITY REQUIREMENTS*) of this Schedule.

5.2 Where the Contractor considers that the obligation in Paragraph 5.1 above conflicts with an obligation contained in any of the standards identified in Schedule 5 (Authority *Standards*), the Contractor shall notify the Authority of such a conflict as soon as it becomes aware of the conflict, and shall follow any guidance provided by the Authority in relation to the same.

5.3 Without prejudice to any shorter timeframes as set out in this Agreement (including as set out in the Authority Standards included in Schedule 5 (Authority *Standards*)), the Contractor shall comply with all cyber security instructions provided by the Authority as soon as reasonably possible.

5.4 The obligations contained in this Schedule shall survive termination or expiry of this Agreement and shall continue in full force and effect at all times whilst Contractor (or any Approved Subcontractor or DCPP Subcontractor) holds MOD Identifiable Information, unless otherwise stated in this Agreement.

6. DCPP REQUIREMENTS

Cyber Risk Level

6.1 The Authority has determined the Cyber Risk Level of this Agreement as "Very Low", as defined in DEFSTAN 05-138.

6.2 The Authority may alter the Cyber Risk Level of this Agreement at any time in its absolute discretion.

DCPP Obligations

6.3 The Contractor shall complete the CSM Risk Assessment Process and CSM Supplier Assurance Questionnaire in accordance with the Authority's instructions.

6.4 The Contractor shall carry out the CSM Supplier Assurance Questionnaire process no less than once in each Contract Year.

DCPP CSM Obligations

6.5 The term "**CSM Subcontractor**" shall mean:

6.5.1 any Approved Subcontractor as defined by Clause 1.1 (*Definitions and Interpretation*);

6.5.2 any subcontractor at any level of the Contractor's supply chain in connection with this Agreement;

6.5.3 any associated company of the Contractor from time to time within the meaning of Section 449 of the Corporation Tax Act 2010;

6.5.4 any parent undertaking or subsidiary undertaking of the Contractor from time to time in accordance with Section 1162 of the Companies Act 2006; and

6.5.5 any subcontractor of such an associated company, parent undertaking or subsidiary undertaking of the Contractor, at any level of the supply chain in connection with this Agreement.

6.6 In relation to each CSM Subcontractor engaged directly by the Contractor, the Contractor shall complete the Cyber Risk Assessment Process in relation to that CSM Subcontractor:

6.6.1 prior to engagement of the CSM Subcontractor;

6.6.2 at least once in each Contract Year; and

6.6.3 otherwise on request by the Authority.

6.7 In relation to each CSM Subcontractor who is not engaged directly by the Contractor ("**Junior CSM Subcontractor**"), the Contractor shall procure that the CSM Subcontractor engaging such a CSM Subcontractor ("**Senior CSM Subcontractor**") completes the Cyber Risk Assessment Process in relation to that Junior CSM Subcontractor:

6.7.1 prior to engagement of the Junior CSM Subcontractor;

6.7.2 at least once in each Contract Year; and

6.7.3 otherwise on request by the Authority,

unless the applicable Cyber Risk Level for the Senior CSM Subcontractor is "not applicable".

6.8 The Contractor shall procure that each CSM Subcontractor which (i) has been subject to the Cyber Risk Assessment Process, and (ii) has a Cyber Risk Level higher than "not applicable" shall be a "**DCPP Subcontractor**", and shall:

6.8.1 comply with DEFSTAN 05-138;

6.8.2 complete a CSM Supplier Assurance Questionnaire at least once in each Contract Year;

6.8.3 implement and maintain all appropriate technical and organisational security measures in accordance with Good Industry Practice to discharge its obligations under this Part C (*CYBER SECURITY REQUIREMENTS*) of this Schedule;

6.8.4 comply with all cyber security instructions provided by the Authority as soon as reasonably possible, subject to any stricter notification requirement set out in this Agreement;

6.8.5 in relation to any Cyber Incident or Other Incident, notify the JSyCC WARP in accordance with ISN 2014/02 as amended or updated from time to time immediately in writing, providing full details or the circumstances of the actual or suspected Cyber Incident or Other Incident which has or may have taken place, providing full details of the circumstances of the Cyber Incident or Other Incident, and any mitigation measures taken or intended to be taken;

6.8.6 investigate any Cyber Incidents or Other Incidents fully and promptly, and cooperate with the Authority, and any Authority agents or representatives, to take all steps to mitigate the impact of the Cyber Incidents or Other Incidents, and to minimise the likelihood of further similar incidents occurring, including complying with any directions of the Authority in relation to the same;

6.8.7 consent to the Authority recording and using information obtained in relation to this Agreement for the purposes of the Cyber Security Model, whether on the Supplier Cyber Protection Service, or elsewhere. For the avoidance of doubt such information may include cyber security accreditation of the CSM Subcontractor; and

6.8.8 include equivalent terms to this Paragraph 6.8 in all of its agreements with its CSM Subcontractor(s) (unless its CSM Subcontractor(s) have a Cyber Risk Level of "not applicable") and where such a CSM Subcontractor breaches such terms, shall in exercising its rights or remedies under the relevant agreement:

(A) notify the Authority of any such breach;

(B) consult with the Authority regarding any remedial or other measures which are proposed as a consequence of such breach; and

(C) act in accordance with the Authority's instructions in relation to such a breach.

6.9 If Contractor becomes aware that a CSM Subcontractor is not able to comply with its obligations under Part C of this Schedule:

6.9.1 the Contractor shall notify the Authority, providing full details of such non-compliance as soon as reasonably practicable and shall consult with the Authority as to the appropriate course of action which may include but shall not be limited to the implementation of a remedial plan or termination of this Agreement with the CSM Subcontractor; and

6.9.2 take all reasonable measures to address any non-compliance of a CSM Subcontractor in accordance with the reasonable timescales proposed by the Authority.

6.10 The Contractor shall be entitled to rely upon self-certification by one or more of its CSM Subcontractor(s) that such a CSM Subcontractor is in compliance with its obligations under Paragraph 6.8 above. In the event that such a CSM Subcontractor is in breach of one or more obligations under Paragraph 6.8 above, and where the Contractor has relied upon that CSM Subcontractor's self-certification in relation to that obligation pursuant to this Paragraph 6.10, the Contractor shall not be held to be in breach of its obligation to procure that CSM Subcontractor's compliance with that obligation under Paragraph 6.8 above.

Cyber Security Implementation Plan

6.11 Where the result of any CSM Supplier Assurance Questionnaire indicates that the Contractor or a DCPP Subcontractor is not able to meet its obligations under this Schedule:

6.11.1 the Authority and the Contractor or DCPP Subcontractor (as applicable) may agree a Cyber Security Implementation Plan; and

6.11.2 the Contractor or DCPP Subcontractor (as applicable) shall comply with such a Cyber Security Implementation Plan.

6.12 In the event that the Contractor has been required by the Authority to implement an agreed Cyber Security Implementation Plan prior to the Contract Date, the Contractor agrees to implement that Cyber Security Implementation Plan (which is annexed hereto) in accordance with its terms.

Terms of Subcontractor Agreements

6.13 The Contractor shall include all terms required to give effect to the obligations contained in this Schedule in its agreements with CSM Subcontractors, and shall procure that such terms are included in all agreements between CSM Subcontractors in the supply chain in connection with this Agreement.

7. RECORDS

7.1 The Contractor shall keep and maintain, and shall ensure that each Subcontractor and DCPP Subcontractor shall keep and maintain:

7.1.1 details of all MOD Identifiable Information; and

7.1.2 copies of all documents required to demonstrate compliance with DEFSTAN 05 – 138 and this Part C of this Schedule, including but not limited to any information used to inform any CSM Risk Assessment Process and to carry out any CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor, Subcontractor or DCPP Subcontractor (as applicable),

in accordance with Schedule 10 (*Records*).

7.2 The Contractor shall, and shall ensure that any Approved Subcontractor or DCPP Subcontractor shall, on request provide to the Authority access to the records referred to in Paragraph 7.1 as may be required in connection with this Agreement.

8. CYBER INCIDENT

8.1 In addition to the Contractor's obligations under Paragraph 4 (*Breach of Security*) of this Schedule above, If the Contractor becomes aware of any actual or suspected:

8.1.1 Cyber Incident; or

8.1.2 any other unauthorised access or use by a third party or misuse, damage or destruction by any person (an "**Other Incident**"),

the Contractor must:

8.1.3 notify the Authority's designated representative immediately; and

8.1.4 comply with any directions issued by the Authority in connection with the Cyber Incident or Other Incident, including in relation to:

(A) obtaining evidence about how, when and by whom the Contractor's information system and/or the Authority Data has or may have been compromised, providing it to the Authority on request, and preserving and protecting that evidence during the Term and for a period of at least six (6) years following the expiry or termination (howsoever arising) of this Agreement;

(B) implementing any mitigation strategies to reduce the impact of the Cyber Incident or Other Incident or the likelihood or impact of any future similar incident;

(C) preserving and protecting Authority Data (including as necessary reverting to any backup or alternative site or taking other action to recover Authority Data); and

(D) investigate any Cyber Incidents or Other Incidents fully and promptly, and cooperate with the Authority, and any Authority agents or representatives, to take all steps to mitigate the impact of the Cyber Incidents or Other Incidents, and to minimise the likelihood of further similar incidents occurring.

8.2 The Contractor must not make or authorise any announcement, other communication or notice about a Cyber Incident (including the giving of a report or notice about a Cyber Incident to any Regulatory Authority) without the prior written consent of the Authority as to the content, media and timing of such an announcement, communication or notice.

8.3 The Contractor must ensure that:

8.3.1 all subcontracts and other supply chain arrangements, which may allow or cause access to Authority Data, contain no provisions that are inconsistent with this Schedule; and

8.3.2 all Contractor Personnel and any Approved Subcontractors or DCPP Subcontractors who have access to Authority Data comply with this Schedule.

8.4 For the avoidance of doubt, no Cyber Incident or Other Incident shall constitute a Force Majeure Event for the purposes of Clause 24 (*Force Majeure*) of this Agreement. If, in the Authority's reasonable opinion, an event has occurred which constitutes a Cyber Incident or Other Incident, the Authority may notify the Contractor that such a Cyber Incident or Other Incident has occurred, and the provisions of Paragraph 4 (*Breach of Security*) and Paragraph 8.1 (*Cyber Incident*) shall apply.

9. CYBER SECURITY GOVERNANCE

9.1 The Contractor shall ensure that all Contractor Personnel who might access the Enterprise IT and Authority Data have received cyber security awareness training and are aware of all applicable security requirements.

9.2 The Contractor shall consent to the Authority recording and using information obtained in relation to this Agreement for the purposes of the Cyber Security Model, whether on the

Supplier Cyber Protection Service, or elsewhere. For the avoidance of doubt such information may include cyber security accreditation of the Contractor.