Defence
Infrastructure
Organisation

Call-Off Schedule 12

ICT Services

Built Estate

REF: RM6089

Version: 1.0 dated 01 Jun 21

CALL-OFF SCHEDULE 12

ICT SERVICES

1. GENERAL

1.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services as part of the Deliverables and the safe use of digital and ICT systems in order to deliver the Services.

2. ADDITIONAL BUYER DUE DILIGENCE REQUIREMENTS

2.1. The Supplier shall satisfy itself of all relevant details, including details relating to the following;

2.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Effective Date) future Operating Environment;

2.1.2. operating processes and procedures and the working methods of the Buyer;

2.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

2.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

2.2. The Supplier confirms that it has advised the Buyer in writing of:

2.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

2.2.2. the actions needed to remedy each such unsuitable aspect; and

2.2.3. a timetable for and the costs of those actions. In accordance with Core Terms Clause 2.8 the Supplier will not be excused of any obligations.

3. WARRANTY OVER LICENSED SOFTWARE

3.1. The Supplier represents and warrants that:

3.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Subcontractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

3.1.2. all components of the Specially Written Software shall:

3.1.2.1. be free from material design and programming errors;

3.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call-Off Schedule 14 (Performance Management) and Documentation; and

3.1.2.3. not infringe any IPR.

4. PROVISION OF ICT SERVICES

4.1. The Supplier shall:

4.1.1. ensure that the release of any new Supplier Software or upgrade to any Supplier Software complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new Supplier Software or Upgrade;

4.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

4.1.3. ensure that the Supplier System will be free of all encumbrances;

4.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

4.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

4.1.6. not release of any new Supplier Software or upgrade to any Supplier Software without the prior written approval of the Buyer, such approval not been unreasonably withheld. The Buyer may request, and the Supplier shall undertake, any reasonable test, including a penetration test with an approved national cyber security centre provider, of the new Supplier Software or upgrade to any Supplier Software prior to approval being provided.

5. STANDARDS & QUALITY REQUIREMENTS FOR ICT SERVICES

5.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

5.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

5.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

5.4. The Supplier shall ensure that the Supplier Staff shall at all times during the Call-Off Contract Period:

5.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

5.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

5.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

6. ADDITIONAL RECORDS AUDIT ACCESS FOR ICT SERVICE CONTRACTS

6.1. The Supplier shall allow any auditor access to the Supplier premises to:

6.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

6.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

6.1.3. review the Supplier's quality management Systems including all relevant Quality Plans.

7. MAINTENANCE OF THE ICT ENVIRONMENT

7.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

7.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule. The Supplier shall ensure that non urgent unplanned maintenance (which shall be known as "**Non Urgent Maintenance**") is added in to the next activity/release date specified in the maintenance schedule.

7.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.

7.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

7.5. The Supplier shall not undertake any maintenance without the prior written approval of the Buyer, such approval not been unreasonably withheld. The Buyer may request, and the Supplier shall undertake, any reasonable test, including a penetration test with an approved national cyber security centre provider, prior to approval being provided.

8. SPECIAL INTELLECTUAL PROPERTY RIGHTS CLAUSE RELATED TO ICT SERVICES

8.1. Assignments granted by the Supplier: Specially Written Software

8.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

8.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

8.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

8.1.2. The Supplier shall:

8.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to Supplier Software or Third Party Software;

8.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in a Mobilisation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the

Buyer and the Buyer shall become the owner of such media upon receipt; and

8.1.2.3. without prejudice to Paragraph 8.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

8.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

8.2. Licences granted by the Supplier: Supplier Software and Supplier Existing IPR

8.2.1. The Supplier hereby grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license:

8.2.1.1. the Supplier Software; and

8.2.1.2. the Supplier Existing IPR,

for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including (in relation to Supplier Software) the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display)).

8.2.2. The Supplier may terminate a licence granted under this Paragraph 8 by giving at least thirty (30) days' notice in writing if there is a Buyer Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

8.3. Buyer's right to assign/novate licences

8.3.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 8.2 (Licences granted by the Supplier: Supplier Software) to:

8.3.1.1. a Central Government Body; or

8.3.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

8.3.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in Paragraph 8.2.

8.4. Third Party IPR and Third Party Software

8.4.1. The Supplier shall procure that the owners or the authorised licensors of any Third Party Software which is not commercial off-the-shelf software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraphs 8.2 and 8.3. If the Supplier cannot obtain such a licence, the Supplier shall:

8.4.1.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

8.4.1.2. only use such Third Party IPR if the Buyer Approves the terms of the licence from the relevant third party.

8.4.2. The Supplier shall procure that the owners or the authorised licensors of any Third Party Software which is commercial off-the-shelf software grants a direct licence to the Buyer on terms no less favourable than those on which such software is usually made available.

8.5. Licence granted by the Buyer

8.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Core Terms Clause 15 (What you must keep confidential).

8.6. Open Source Publication

8.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to Paragraph 8.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

8.6.1.1. suitable for publication by the Buyer as Open Source; and

8.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

8.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

8.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

8.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

8.6.2.3. do not contain any material which would bring the Buyer into disrepute;

8.6.2.4. can be published as Open Source without breaching the rights of any third party;

8.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified to by the Buyer to the Supplier; and

8.6.2.6. do not contain any Malicious Software.

8.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

8.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

8.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

8.7. Malicious Software

8.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an

industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

8.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

8.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 8.7.2 shall be borne by the Parties as follows:

8.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

8.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

9. CYBER

9.1. The Buyer shall:

9.1.1. determine the Cyber Risk Level appropriate to this Contract and, where the Supplier 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 Supplier as soon as is reasonably practicable; and

9.1.2. notify the Supplier as soon as reasonably practicable where the Buyer reassesses the Cyber Risk Level relating to this Contract.

9.2. The Supplier shall, and shall procure that its Subcontractors shall:

9.2.1. comply with DEFSTAN 05-138;

9.2.2. complete the Cyber Security Model (CSM) Risk Assessment Process in accordance with the Buyer's instructions, ensuring that any change in the Cyber Risk Level is notified to any affected Subcontractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Supplier'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 Buyer;

9.2.3. 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;

9.2.4. having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge its obligations under this Paragraph in accordance with Good Industry Practice provided always that where there is a conflict between the Supplier's obligations under Paragraph 10.2.1 above and this Paragraph 10.2.4, the Supplier shall notify the Buyer in accordance with the notification provisions in DEFSTAN 05-138 as soon as it becomes aware of the conflict and the Buyer shall determine which standard or measure shall take precedence;

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

9.2.6. notify the JSyCC WARP in accordance with ISN 2014/02 as amended or updated from time to time and the Supplier's National or Designated Security Advisor (NSA/DSA), and in the case of a Subcontractor also notify the Supplier, 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;

9.2.7. in coordination with its NSA/DSA, investigate any Cyber Security Incidents fully and promptly and co-operate with the Buyer 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 Supplier's NSA/DSA in the circumstances and taking into account the Cyber Risk Level; and

9.2.8. consent to the Buyer 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 Supplier and / or Subcontractor as appropriate; and

9.2.9. include provisions equivalent to Paragraph 10.5 in all Subcontracts imposing provisions equivalent to Paragraph 10.2 (the "equivalent provisions") and, where a Subcontractor breaches terms implementing this Paragraph in a Sub-Contract, the Supplier shall,

and shall procure that its Subcontractors shall, in exercising their rights or remedies under the relevant Sub-Contract:

9.2.9.1. notify the Buyer of any such breach and consult with the Buyer regarding any remedial or other measures which are proposed as a consequence of such breach, taking the Buyer's views into consideration; and

9.2.9.2. have regard to the equivalent provisions. PROVIDED ALWAYS THAT where the Supplier has notified the Buyer that it or one or more if its Subcontractors cannot comply with Paragraphs 9.2.1 to 9.2.9 above the Buyer and Supplier will seek to agree a Cyber Security Implementation Plan and where the Buyer has agreed a Cyber Security Implementation Plan with the Supplier, the Supplier shall, and shall procure that its Subcontractors shall, comply with such Cyber Security Implementation Plan until implementation is agreed to have been achieved whereupon Paragraphs 9.2.1 to 9.2.9 above shall apply in full. In the event that a Cyber Security Implementation Plan cannot be agreed the Dispute Resolution Procedure shall apply.

9.3. Management Of Sub-Contractors

9.3.1. The Buyer agrees that the Supplier shall be entitled to rely upon the self-certification by a Subcontractor of its compliance with its obligations pursuant to Paragraph 9.2. In the event that a Subcontractor is found to be in breach of its obligations in Paragraph 9.2, and where the Supplier has relied upon the Subcontractor's self-certification, the Supplier shall not be held to be in breach of this Condition.

9.3.2. Where the Supplier becomes aware that a Subcontractor is not complying with its obligations, the Supplier shall notify the Buyer and provide full details of the Subcontractor's non-compliance as soon as reasonably practicable and shall consult with the Buyer as to the appropriate course of action which may include but not be limited to the agreement of a remedial plan or termination of the Sub-Contract having regard to Paragraph 9.2.9.

9.3.3. Having regard to the Buyer's views, the Supplier shall take all reasonable measures to address any non-compliance of a Subcontractor in accordance with the reasonable timescales required by the Buyer. Where the Supplier fails to do so, this shall

amount to a breach of this Paragraph and the provisions of Paragraphs 9.5.2 or 9.5.3 as appropriate shall apply.

9.3.4. The Supplier shall, and shall procure that its Subcontractors shall, include provisions in all Sub-Contracts which flow down the obligations set out in Paragraph 9.2 of this Schedule.

9.4. Audit

9.4.1. Except where an audit is imposed on the Buyer by a regulatory body, or there is a Cyber Security Incident, in which case the Supplier agrees and shall procure that its Subcontractors agree, that the Buyer and its representatives in coordination with the Supplier's NSA/DSA or the NSA/DSA on behalf of the Buyer, may conduct such audits as it considers in its absolute opinion necessary; the Buyer, its representatives and/or the Supplier's 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:

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

9.4.1.2. to review the Supplier's and/or any Subcontractor's compliance with its obligations under Paragraph 9; and

9.4.1.3. to review any records created during the provision of the Deliverables, including but not limited to any documents, reports and minutes which refer or relate to the Deliverables for the purposes of Paragraphs 9.4.1.1 and 9.4.2.2 above.

9.4.2. The Buyer shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier and/or Subcontractor or delay the provision of the Deliverables and supplier information received by the Buyer in connection with the audit shall be treated as Confidential Information.

9.4.3. The Supplier shall, and shall ensure that any Subcontractor shall on demand provide the Buyer and any relevant regulatory body, including the Supplier'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:

9.4.3.1. all information requested by the Buyer within the permitted scope of the audit;

9.4.3.2. reasonable access to any Sites controlled by the Supplier or any Associated Company and any Subcontractor 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 Supplier, shall

secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

9.4.3.3. access to any relevant staff.

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

9.4.5. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Paragraph, unless the audit identifies a material breach of the terms of this Paragraph by the Supplier and/or Subcontractor in which case the Supplier shall reimburse the Buyer for all the Buyer's reasonable costs incurred in the course of the audit.

9.5. Breach of Obligations

9.5.1. In exercising its rights or remedies under this Paragraph, the Buyer shall:

9.5.1.1. 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

9.5.1.2. 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.

9.5.2. Where the Cyber Risk Level of this Contract is assessed to be a moderate or high Cyber Risk Level in the CSM, and the Supplier breaches the terms of this Paragraph, the Buyer shall be entitled:

9.5.2.1. to terminate the Contract (whether in whole or in part) and to claim damages on the basis that such breach is a material breach in accordance with Clause 10.4 of the Core Terms; and

9.5.2.2. where the Contract has not been terminated, to recover from the Supplier any other loss sustained in consequence of any

breach of this Paragraph, subject to any provision which is agreed elsewhere in this Contract.

9.5.3. Where the Cyber Risk Level of this Contract is assessed to be very low or low, and the Supplier breaches the terms of this Paragraph, the Buyer shall be entitled:

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

9.5.3.2. where the Supplier does not comply with any reasonable instructions issued by the Buyer or the Supplier's NSA/DSA within the time period specified to remedy such breach or prevent further breaches, the Buyer shall be entitled to terminate this Contract (whether in whole or in part) and to claim damages on the basis that such breach is a material breach.

9.5.4. Where the Supplier commits an act of fraud, negligence or wilful misconduct in respect of its obligations under this Paragraph the Buyer shall be entitled to terminate this Contract (whether in whole or in part) and to claim damages on the basis that such breach is a material breach.

9.6. General

9.6.1. On termination or expiry of this Contract the provisions of this Paragraph excepting Paragraphs 9.2.2 and 9.2.3 above shall continue in force so long as the Supplier and/or and Subcontractor holds any MOD Identifiable Information relating to this Contract.

9.6.2. Termination or expiry of this Contract shall not affect any rights, remedies, obligations or liabilities of the Parties under this Paragraph 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.

9.6.3. The Supplier agrees that the Buyer 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 Charges for any associated increase or decrease in costs and the Supplier may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Cyber Risk Level provided always that the Supplier 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.

9.6.4. The Supplier shall not recover any costs and/or other losses under or in connection with this Paragraph where such costs and/or other losses are recoverable or have been recovered by the Supplier 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 Supplier 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 Supplier and the Buyer or with other bodies.

Annex: Software

SUPPLIER SOFTWARE

[Redacted – Commercially Sensitive]