

Call-Off Schedule 1 (Transparency Reports)

- 1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>)). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
- 1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
- 1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
- 1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Publication of the Contract for Transparency Purposes	The content of the contract in its entirety excluding commercially sensitive information declared by the supplier in Joint Schedule 4.	PDF to be published on Contracts Finder	One at contract award. Following any contract amendments.

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

- 1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2. Supplier's Obligations

- 2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.
- 2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.
- 2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year ("**Continuous Improvement Plan**") for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:
 - 2.3.1 identifying the emergence of relevant new and evolving technologies;
 - 2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);
 - 2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and
 - 2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.
- 2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.
- 2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised

- Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.
- 2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
 - 2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
 - 2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
 - 2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
 - 2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
 - 2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
 - 2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.
 - 2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
 - 2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 4 (Call Off Tender)

[REDACTED]

Call-Off Schedule 6 (ICT Services)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

- "Buyer Property"** the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
- "Buyer Software"** any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
- "Buyer System"** the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
- "Defect"** any of the following:
- a) any error, damage or defect in the manufacturing of a Deliverable; or
 - b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or
 - c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or
 - d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant

Deliverable from passing any Test required under this Contract;

"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
"Maintenance Schedule"	has the meaning given to it in paragraph 8 of this Schedule;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or

- b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or
- c) where any part of the Supplier System is situated;

"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

- 2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT services which are part of the Deliverables.

3. Buyer due diligence requirements

- 3.1. This paragraph 3 applies where the Buyer has conducted a Further Competition. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
 - 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
 - 3.1.2. operating processes and procedures and the working methods of the Buyer;
 - 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
 - 3.1.4. 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.
- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
 - 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the Deliverables;
 - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3. a timetable for and the costs of those actions.

4. Software warranty

- 4.1. The Supplier represents and warrants that:
 - 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) 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;
 - 4.1.2. all components of the Specially Written Software shall:
 - 4.1.2.1. be free from material design and programming errors;
 - 4.1.2.2. perform in all material respects in accordance with the relevant specifications and Documentation; and
 - 4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

- 5.1. The Supplier shall:

- 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with any interface requirements of the Buyer specified in this Contract 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 COTS Software or Upgrade;
- 5.1.2. 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;
- 5.1.3. ensure that the Supplier System will be free of all encumbrances;
- 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
- 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1. The Supplier shall, where specified by the Buyer as part of their Further Competition, and in accordance with agreed timescales, develop 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**").
- 6.2. 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.
- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
 - 6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
 - 6.4.2. 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
 - 6.4.3. 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.

7. ICT Audit

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

- 7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);
- 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
- 7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer undertaking a Further Competition, 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.
- 8.2. 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.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
- 8.4. 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.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

- 9.1.1. 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:
 - 9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - 9.1.1.2. 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**").
- 9.1.2. The Supplier shall:
 - 9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

- 9.1.2.2. 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 an Implementation 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
 - 9.1.2.3. without prejudice to paragraph 9.1.2.2, 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.
- 9.1.3. 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.
- 9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer**
- 9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:
 - a) of its own Existing IPR that is not COTS Software;
 - b) third party software that is not COTS Software
 - 9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same 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 the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.
 - 9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the

authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. 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

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority 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.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. 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.

9.4.2. 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 9.2.

9.5. Licence granted by the Buyer

9.5.1. 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 Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) 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:

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

9.6.1.2. based on Open Standards (where applicable),

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

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

9.6.2.1. 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;

9.6.2.2. 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;

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

- 9.6.2.4. can be published as Open Source without breaching the rights of any third party;
 - 9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
 - 9.6.2.6. do not contain any Malicious Software.
- 9.6.3. 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:
- 9.6.3.1. 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
 - 9.6.3.2. 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.

9.7. Malicious Software

- 9.7.1. 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.
- 9.7.2. 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 Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.
- 9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
 - 9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government 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

9.7.3.2. 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).

10. Supplier-Furnished Terms

10.1. Software Licence Terms

10.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Annex A of this Call-Off Schedule 6.

10.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call-Off Schedule 6.

10.2. Software Support & Maintenance Terms

10.2.1.1. Additional terms for provision of Software Support & Maintenance Services are detailed in Annex C of this Call-Off Schedule 6.

10.3. Software as a Service Terms

10.3.1.1. Not applicable

10.4. Device as a Service Terms

10.4.1.1. Not applicable

11. CUSTOMER PREMISES

11.1 Licence to occupy Customer Premises

11.1.1 Any Customer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Call- Off Contract. The Supplier shall have the use of such Customer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract [and in accordance with Call-Off Schedule 10 (Exit Management)].

11.1.2 The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

11.1.3 Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call Off Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any

modification work which it approves pursuant to this paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

11.1.4 The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

11.1.5 The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

11.2 Security of Buyer Premises

11.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

11.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

12. Buyer Property

12.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

12.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

12.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

12.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

12.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.

12.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call- Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

12.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

13. Supplier Equipment

13.1 Unless otherwise stated in this Call Off Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

13.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

13.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

13.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

13.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

13.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

13.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

13.7.1 remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

13.7.2 replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

ANNEX A

Non-COTS Third Party Software Licensing Terms

1. The Supplier shall make any modifications to the system solely for the use of the Buyer and will not offer these modifications commercially without authority from the Buyer.

ANNEX B

COTS Licensing Terms

1. The Supplier shall make any modifications to the system solely for the use of the Buyer and will not offer these modifications commercially without authority from the Buyer.

ANNEX C

Software Support & Maintenance Terms

1. The supplier shall provide annual software maintenance and through life support in order to ensure the software operates without issues.
2. Software updates and patches shall be provided to the Buyer according to the priority of the update/patch. Updates shall be provided at no additional charge and may be delivered via physical media or made available through electronic means.

Normal

Measures:- Routine Computer Network Defence measures appropriate to the business and systems concerned.

Related Threat Levels:- Low and Moderate

Heightened

Measures:- Additional and sustainable Computer Network Defence measures reflecting the broad nature of the threat combined with specific business and system vulnerabilities and judgements on acceptable risk.

Related Threat Levels:- Substantial and Severe

Exceptional

Measures:- Maximum protective security measures to meet specific threats and to minimise vulnerability and risk.

Related Threat Levels:- Critical

Patch Type	Timeframe
Normal	Within 1 month
Heightened	Within 1 week
Exceptional	Within 1 day

ANNEX D

Software as a Service Terms

Not applicable

Annex E

Device as a Service Terms

Not applicable

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

PART B: SHORT FORM BUSINESS CONTINUITY & DISASTER RECOVERY

1. The Supplier's business continuity and disaster recovery plan is appended at Annex 1 hereto.
2. The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier if required at no additional cost to the Buyer.
3. If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

ANNEX 1

[REDACTED]

Call-Off Schedule 9 (Security)

Part B: Long Form Security Requirements

1. Definitions

1.1 In this Schedule the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 Head of SBA Customs & Immigration

2.3.2 Contract Administrator

2.4 The Buyer shall clearly articulate its high-level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer

Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph **Error! Reference source not found.**;

3.4.3 at all times provide a level of security which:

- (a) is in accordance with the Law and this Contract;
- (b) complies with the Baseline Security Requirements;
- (c) as a minimum demonstrates Good Industry Practice;
- (d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
- (e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)
(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
- (f) takes account of guidance issued by the Centre for Protection of National Infrastructure
(<https://www.cpni.gov.uk>)
- (g) complies with HMG Information Assurance Maturity Model and Assurance Framework
(<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>)
- (h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
- (i) addresses issues of incompatibility with the Supplier's own organisational security policies; and
- (j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph **Error! Reference source not found.**;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph **Error! Reference source not found.** fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

- 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
- 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- 4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
- 4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- 4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
- 4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);
- 4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
- 4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

- 5.2.2 updates to the risk assessments;
 - 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 5.2.4 suggested improvements in measuring the effectiveness of controls.
- 5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex **1** (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system

management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- (a) minimise the extent of actual or potential harm caused by any Breach of Security;
- (b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
- (c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;
- (d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
- (e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
- (f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

- 9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
 - 9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;
 - 9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;
 - 9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;
 - 9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
 - 9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and
 - 9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.
- 9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
- 9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

- 4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.
- 4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

- 5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
- 5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (<https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[REDACTED]

Call-Off Schedule 10 (Exit Management)

Part B: Short Form Exit Management Requirements

1. Within 20 (twenty) working days of the Start Date the Supplier must provide the Buyer with an exit plan which ensures continuity of service and which the Supplier will follow.

2 The Supplier must ensure that the exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the contract ends before the scheduled expiry.

3 The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for export and migration of Buyer data from the Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of project- specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which are reasonably required to ensure continuity of Service during the exit period and an orderly transition

4. When requested, the Supplier will help the Buyer to migrate the Services to a Replacement Supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract ended before the Expiry Date due to Supplier cause. Otherwise any additional costs incurred by the Supplier in providing such assistance shall be subject to the Variation Procedure.

Call-Off Schedule 11 (Installation Works)

11. When this Schedule should be used

11.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of Deliverables requiring installation by the Supplier.

12. How things must be installed

12.1. Where the Supplier reasonably believes, it has completed the Installation Works it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:

12.1.1. accept the Installation Works, or

12.1.2. reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).

12.2. If the Buyer rejects the Installation Works in accordance with Paragraph 2.1.2, the Supplier shall immediately rectify or remedy any defects and if, in the Buyer's reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.

12.3. The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.1.1. Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.1, the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

12.4. Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A – Implementation Plan

1. Agreeing the Implementation Plan

- 1.1 The Supplier's tendered draft Implementation Plan is at Annex 1 to this Part A of Call-Off Schedule 13. The Supplier will provide an updated, fully developed draft for Approval within 15 working days of the Call-Off Contract Start Date.
- 1.2 The updated draft must contain enough detail for effective management of Contract implementation.
- 1.3 The Buyer shall not unreasonably withhold Approval of the updated draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it.

2. Following the Implementation Plan

- 2.1 The Supplier shall perform its obligations in respect of Delivery and, where relevant, Testing of the Deliverables in accordance with the Approved Implementation Plan.
- 2.2 Changes to any Milestones, Milestone Dates, Milestone Payments or Delay Payments shall only be made via the Variation Procedure.
- 2.3 Where the Supplier is responsible for the failure to achieve a Milestone by the date specified in the Approved Implementation Plan this shall constitute a material Default.

3. Delays

- 3.1 If the Supplier becomes aware that there is, or is likely to be, a Delay it shall;
 - Notify the Buyer in writing within 2 Working Days of becoming aware, explaining the likely impact of the Delay
 - Use all reasonable endeavours to mitigate the effects of the Delay, including complying with the Buyer's reasonable instructions

4. Delay Payments

- 4.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Buyer

shall deduct the relevant Delay Payments before processing payment for the relevant milestone.

Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to achieve a Milestone by its Milestone Date except where:

- (a) the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or
- (b) the delay exceeds the number of days (the "Delay Period Limit") specified in the Contract commencing on the relevant Milestone Date;

The Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is achieved;

No payment or other act or omission of the Buyer shall affect the Buyer's right to recover the Delay Payments, or be deemed to be a waiver of the right of the Buyer to recover any such damages;

4.2 Milestones, Delay Payment Rates and Period Limits are listed below.

Milestone	Daily Rate	Period Limit
Deployment and installation of scanners at all locations.	[REDACTED]	None
All Superusers users to be provided with Train the Trainer Training.	[REDACTED]	None

Call-Off Ref: 701553520
Crown Copyright 2019

Annex 1 Draft Implementation Plan

[REDACTED]

Part B – Testing

In this Part B to Call-Off Schedule 13, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Test Plan"	a plan for the Testing of the Deliverables to demonstrate compliance with Contract requirements;
"Test Report"	a test report produced by the Supplier in accordance with Paragraph 3.3 of this Part B to Call-Off Schedule 13;

- 1.1 All Tests will be carried out in accordance with the Test Plan.
- 1.2 The Supplier shall submit each Deliverable for the relevant Testing no later than the date specified in the Contract for the Test Period to begin.
- 2.1 The Supplier shall submit a draft Test Plan for Approval no later than 28 days after the Start Date.
- 2.2 The Test Plan will include:
 - An overview of how Testing will be carried out
 - Specific details of each Test to be carried out to demonstrate that the Buyer's requirements are satisfied
 - The Test Success Criteria for all Tests
 - A timetable for Testing over the Test Period, this to be compliant with any Implementation Plan
 - The process for recording the conduct and results of Testing
 - The responsibilities of the Parties
 - A categorisation scheme for test issues eg critical/serious/minor
- 2.3 The Buyer shall not unreasonably withhold Approval of the Test Plan provided that the Supplier shall implement the Buyer's reasonable requirements in the plan.
- 3.1 Unless specified in the Test Plan the Supplier shall be responsible for carrying out the Testing detailed in the plan.
- 3.2 The Buyer may require that a Buyer representative witnesses the conduct of the Tests.
- 3.3 No later than 10 days after the completion of the scheduled Test Period the Supplier shall provide the Buyer with a Test Report setting out:
 - An overview of Testing carried out

- Details of each Test carried out together with the result, indicating if the success criteria were satisfied
 - Details of any scheduled Tests that were not carried out
 - A list of all outstanding Test issues
- 4.1 Where by the end of the scheduled Test Period the Testing process has demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer shall notify the Supplier in writing that the Testing process has been satisfactorily completed.
- 4.2 Where as a result of a Supplier default the Testing process has not by the end of the scheduled Test Period demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer may:
- Direct the Supplier to repeat any unsuccessful Test or undertake any scheduled Test not thus far undertaken to give the Supplier an opportunity to demonstrate that the outstanding issues detailed in the Test Report have been resolved; or
 - Notify the Supplier that testing has been satisfactorily completed subject to rectification of outstanding issues within a period specified by the Buyer. Failure to rectify the relevant issues within the period specified shall be a material Default; or
 - to reject the relevant Deliverables and to invoke Clause 3.2.12; or
 - to reject the relevant Deliverables treating this as a material default and invoking the Buyer's termination right under Clause 10.4.1

Call-Off Ref: 701553520
Crown Copyright 2019

Example Test Plan

[REDACTED]

Call-Off Schedule 14 (Service Levels)

Definitions

In this Part Call-Off Schedule 14, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Performance Monitoring Report"	Means a Performance Monitoring Report as specified by Section 3 of this Call-Off Schedule 14
"Service Credits"	any service credits specified in the Annex to Section 2 of this Call-Off Schedule 14 being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Annex to Section 2 of this Call-Off Schedule 14
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Section 2 of this Call-Off Schedule 14; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Section 2 to this Call-Off Schedule 14
"Service Level Period"	means 3 months/quarterly (starting from the date of contract commencement)

9. What happens if you don't meet the Service Levels

- 9.1 The Supplier shall at all times provide the Deliverables to meet the Service Level Performance Measure for each Service Level.
- 9.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Section 2 to this Schedule 14 including the right to any Service Credits, which are a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.
- 9.3 The Supplier shall send Performance Monitoring Reports to the Buyer in accordance with the provisions of Section 3 (Performance Monitoring) of this Call-Off Schedule 14.
- 9.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

- 9.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
- 9.4.2 the Service Level Failure:
 - (a) exceeds the relevant Service Level Threshold;
 - (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;
 - (c) results in the corruption or loss of any Government Data; and/or
 - (d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or
- 9.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

Section 2: Service Levels and Service Credits

1. Service Levels

- 1.1 If the level of performance of the Supplier is likely to or fails to meet any Service Level Performance Measure the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:
 - 1.1.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer;
 - 1.1.2 instruct the Supplier to comply with the Rectification Plan Process;
 - 1.1.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
 - 1.1.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

- 1.2 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.
- 1.3 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Section 2 of this Call-Off Schedule 14.

ANNEX 1 TO SECTION 2: SERVICES LEVELS AND SERVICE CREDITS TABLE

Monitoring of KPI/SLAs and application of service credits shall only come into effect once the system has been installed.

KPI/SLA Ref No	Service Level Performance Criterion	Response Required	Service Level Performance Measure	Service Credit/Delay Payments
1	24/7/365 telephone support for Full system outage impacting on all systems. No alternative solutions can be found.	First attempt dial, call answered within 1 minute. Technical support offered within 1 hour.	At least 100% at all times.	
2	24-hour response to Partial system failure. Some systems are operational, but outputs are affected. Processing of data can continue but is limited and causing delays.	Onsite or remote technical support provided within 24 hours of the initial incident.	at least 100% at all times	
3	48-hour response to System performance issues where the system is operational, but performance is reduced. Minor delays to processing data.	Onsite or remote technical support provided within 48 hours of the initial incident.	at least 100% at all times	
4	5-day response to minor system errors that are not affecting performance of the system	Onsite or remote technical support provided within 5 calendar days of the initial incident.	at least 100% at all times	
5	Software and security patch updates to be supplied according to timeframes within Schedule 6 – ICT Services	Software updates to be tested and installed by the Supplier	at least 100% at all times	
6	Maintain at least 2 operational scanning devices at each of the 3 locations (Pergamos Crossing Point,	Additional spare scanning devices to remain in reserve on island (Cyprus) to ensure minimum units	at least 100% at all times	0.5% Service Credit gained for each percentage under the

	Strovia Crossing Point & RAF Akrotiri)	at each location can be maintained. Scanning devices that become non-operational are to be replaced by a reserve within 24 hours.		specified Service Level Performance Measure
7	Maintain at least 1 operational scanning device at each of the 3 locations (Pergamos Crossing Point, Strovia Crossing Point & RAF Akrotiri)	Additional spare scanning devices to remain in reserve on island (Cyprus) to ensure minimum units at each location can be maintained.	at least 100% at all times	2% Service Credit gained for each percentage under the specified Service Level Performance Measure

Service credits have been allocated to those KPI/SLAs seen as critical, however the supplier should note the Authority will monitor performance against all KPI/SLAs to ensure the supplier is delivering the service as required.

The Service Credits shall be calculated on the basis of the following formula:

Formula: $x\%$ (Service Level Performance Measure) - $x\%$ (actual Service Level performance) = $x\%$ of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance) = 23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

achieved against this Service
Level in a Service Period)

“Service Credit Cap” means:

In the period from the Call-Off Commencement Date to the end of the first Call-Off Contract year ten per cent 10% of the charges payable to the supplier; and

During the remainder of the Call-Off Contract Period, thirty five per cent (35%) of the Call-Off Contract Charges payable to the Supplier under this Call-Off Contract in the period of twelve (12) Months immediately preceding the Month in respect of which Service Credits are accrued;

Section 3: Performance Monitoring

10. Performance Monitoring and Performance Review

- 1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of the proposed process for monitoring and reporting of Service Levels, and the Parties will try to agree the process as soon as reasonably possible.
- 1.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") as agreed pursuant to paragraph 1.1 above which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
 - 1.2.1 for each Service Level, the actual performance achieved over the relevant Service Period;
 - 1.2.2 a summary of all failures to achieve Service Levels;
 - 1.2.3 details of any Critical Service Level Failures;
 - 1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
 - 1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
 - 1.2.6 such other details as the Buyer may reasonably require .
- 1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Quarterly basis to review by Performance Monitoring Reports. The Performance Review Meetings shall :
 - 1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued at such location and time (within normal business hours) as the Parties may agree;
 - 1.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 1.3.3 be fully minuted by the Supplier, with the minutes circulated by to all attendees at the relevant meeting and also any other recipients agreed at the relevant meeting.

The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

Call-Off Schedule 17 (MOD Terms)

1 Definitions

- 1.1 This Schedule 17 shall be incorporated into all Call-Off Contracts placed by the Ministry of Defence
- 1.2 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):
- | | |
|-----------------------------------|---|
| "MOD Terms and Conditions" | the terms and conditions listed in this Schedule; |
| "MOD Site" | shall include any of Her Majesty's Ships or Vessels and Service Stations; |
| "Officer in charge" | shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments; |
- 1.3 **Supplying to the Ministry of Defence-** the Supplier shall comply with all specified MOD additional terms where required. MOD source of CCS catalogue content is Basware Government eMarketplace. Orders, invoice and payment will be transacted through the Contracting Purchasing and Finance payment system.

2 Access to MOD sites

- 2.1 The Buyer shall issue passes for those representatives of the Supplier who are approved for admission to the MOD Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Buyer and shall be surrendered on demand or on completion of the supply of the Deliverables.
- 2.2 The Supplier's representatives when employed within the boundaries of a MOD Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of staff at that MOD Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.
- 2.3 The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a MOD Site. Sleeping accommodation and messing facilities, if required, may be provided by the Buyer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At MOD Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's staff for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his

decision before the commencement of this Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Buyer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Buyer with other evidence relating to the costs of this Contract.

- 2.4 Where the Supplier's representatives are required by this Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in the Buyer Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Buyer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is necessary for the purpose of this Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.
- 2.5 Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.
- 2.6 Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc. Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.
- 2.7 No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.
- 2.8 The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Buyer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to

which the Supplier's representatives are attached. All such advances made by the Buyer shall be recovered from the Supplier

3 DEFCONS and DEFFORMS

- 3.1 The DEFCONS and DEFORMS listed in Annex 1 to this Schedule are incorporated into this Contract. Where a DEFCON or DEFORM is updated or replaced the reference below shall be taken as referring to the updated or replacement DEFCON/DEFORM.
- 3.2 In the event of a conflict between any DEFCONS and DEFFORMS listed in the Order Form and the other terms in a Call Off Contract, the DEFCONS and DEFFORMS shall prevail.

ANNEX 1 - DEFCONS & DEFFORMS

The full text of Defence Conditions (DEFCONS) and Defence Forms (DEFFORMS) are available electronically via <https://www.gov.uk/acquisition-operating-framework>.

The following MOD DEFCONS and DEFFORMs form part of this contract:

DEFCONS

DEFCON No	Version	Description
Applicable to all Lots:		
DEFCON 5J	18/11/16	Unique Identifiers – Clause 4 does not apply
DEFCON 68	05/21	Supply Of Data For Hazardous Articles, Material and Substances
DEFCON 76	06/21	Contractors Personnel At Government Establishments
DEFCON 90	06/21	Copyright
DEFCON 129J	18/11/16	The Use Of Electronic Business Delivery Form
DEFCON 516	04/12	Equality
DEFCON 520	05/18	Corrupt Gifts And Payments Of Commission
DEFCON 522	11/17	Payment And Recovery Of Sums Due
DEFCON 531	11/14	Disclosure Of Information
DEFCON 658	10/17	Cyber – Further to DEFCON 658 the Cyber Risk Profile for this Contract is High, as defined in Def Stan 05-138.
DEFCON 659A	02/17	Security Measures

DEFFORMs (Ministry of Defence Forms) – None Required

DEFFORM No	Version	Description
------------	---------	-------------

Call-Off Schedule 18 (Background Checks)

11. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

12. Definitions

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

13. Relevant Convictions

13.1.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

13.1.2 Notwithstanding Paragraph 2.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

- (a) carry out a check with the records held by the Department for Education (DfE);
- (b) conduct thorough questioning regarding any Relevant Convictions; and
- (c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

You must tell us about unspent convictions under the:

Immigration Act 1971

Asylum & Immigration Act 1996

Nationality, Immigration & Asylum Act 2002

Asylum and Immigration (TOC etc.) Act 2004

Immigration, Asylum and Nationality Act 2006

Accession (Immigration and Worker Registration) Regulations 2006 (SI 2006/3317)

United Kingdom Borders Act 2007

Borders, Citizenship and Immigration Act 2009

Forgery & Counterfeiting Act 1981

Identity Cards Act 2006

Sexual Offences Act 2003

Customs and Excise Management Act 1979

Commissioners for Revenue and Customs Act 2005

Data Protection Act 2018

Fraud Act 2006

Any equivalent offences under relevant legislation in Cyprus.

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

STATEMENT OF REQUIREMENTS

1 INTRODUCTION AND BACKGROUND TO THE AUTHORITY

- 1.1 The Sovereign Base Area Administration (SBAA) operates Customs and Immigration controls at a single airhead (RAF Akrotiri) and two vehicle crossing points on the island of Cyprus.
- 1.2 The SBAA is funded by the Ministry of Defence (MOD) and are seeking one supplier for the provision of a networked passport scanning solution at three (3) locations in Cyprus.
- 1.3 Sovereign Base Area Customs & Immigration (SBA C&I) are an operational law enforcement agency of the SBAA who provide 24/7 border security at crossing points and within the air terminal.
- 1.4 The two land crossing points are located within the Eastern Sovereign Base Area in Cyprus. 2019 saw 1.4 million persons crossing at SBA crossing points. Both crossing points are located on the boundary between the SBA and the Turkish Controlled Area (TCA) of Cyprus.
- 1.5 SBA C&I also operate Immigration controls at RAF Akrotiri processing approximately 30,000 passengers' arrivals each year.
- 1.6 MOD may be referred to as the Authority / Contracting Authority for the remainder of this document.

2 OVERVIEW OF REQUIREMENT

- 2.1 The Authority requires an ID and passport scanning solution for its border entry points, of a similar standard to those used in the UK and Cyprus at official entry points (airports / seaports etc.) with an integrated information management system.
- 2.2 Definitions:

Expression or Acronym	Definition
SBAA	Sovereign Base Areas Administration. The governing body of the UK owned Sovereign Base Area
SBA	Sovereign Base Area. The areas under UK sovereignty in Cyprus
ESBA	Eastern Sovereign Base Area and covers Dhekelia and Ayios Nicolaos.
WSBA	Western Sovereign Base Area and covers Akrotiri and Episkopi.
TCA	Turkish Controlled Area. The area of Northern Cyprus which is under Turkish control since 1974.

MRZ	Machine Readable Passport
SBA C&I	Sovereign Base Area's Customs & Immigration. The law enforcement agency responsible for SBA borders.
ICAO	International Civil Aviation Organisation
EAC	Extended Access Control
RFID	Radio-frequency Identification
BAC	Basic Access Control
SAC	Supplemental Access Control
PACE	Password Authenticated Connection Establishment
IR	Infra-Red
UV	Ultraviolet
ICAO 9303	International Civil Aviation Organisation specifications on machine readable travel documents.

3 SPECIFICATION

3.1 The Authority is seeking the provision of a Passport Scanning solution and support for a period of 5 years from September 2021 to September 2026 (this may change dependant on the completion of system installation).

Outline of the requirement stating what is in and out of scope of the MOD's requirements:

3.1.1 In scope:

3.1.1.1 Passport scanning solution for the SBA to check and record passport and national identity cards.

3.1.1.2 Able to read non MRZ documents.

3.1.1.3 Fully integrated passport scanning solution including hardware and software requirements.

3.1.1.4 Software support and maintenance.

3.1.2 Out of scope:

3.1.2.1 Cloud based system

3.1.3 Mandatory:

3.1.3.1 System must be networked across three (3) sites (Pergamos Check Point, Strovilia Check Point and RAF Akrotiri) with a computer terminal located in the WSBA (M1 Police Station) capable of accessing the system.

3.1.3.2 Data must be suitably encrypted

3.1.3.3 Interoperability with other systems

3.1.3.4 Compliant with UK GDPR regulations inclusive of any changes for the life of the contract

The Requirement

3.2 The following provides the statement of requirements for the scanners:

- 3.2.1 Compact full-page document scanner
- 3.2.2 Able to read machine readable documents in under five (5) seconds
- 3.2.3 Read ePassports (BAC, SAC, EAC, PACE, RFID), ID cards, visas and national identity cards.
- 3.2.4 Reads ICAO compliant documents as well as non-compliant travel documents
- 3.2.5 Operate in zero (0) to fifty (50) degree Celsius temperature range
- 3.2.6 Dust sealed and rated to IP50
- 3.2.7 ICAO 9303 checksum, IR ink and UV dull validation checks
- 3.2.8 Cross check of photo in chip to photo in document
- 3.2.9 Security lock to prevent theft of the scanner
- 3.2.10 Hardware required for the passport scanning solution to be security protected, e.g. non-essential USB locked, non-essential apps and software disabled.
- 3.2.11 Suppliers should note the requirement for additional devices in order to achieve KPI/SLAs outlined in call-off schedule 14 – Service levels.

3.3 The following provides the statement of requirements for the software/interface:

- 3.3.1 End to end encryption of data (Minimum Advanced Encryption Standard AES-256)
- 3.3.2 Searches against multiple watchlist data and provide operating officer(s) feedback
- 3.3.3 Able to send alerts to user when passport has a stop or report action
- 3.3.4 Ability to send discreet markers to data owners without alerting the officer that the person is on a watchlist.
- 3.3.5 Function to enable users to manually input where a document fails to read on the scanner. Where manual searches are entered the system can record what users are searching to mitigate against misuse.

- 3.3.6 Records all entries whether being read from the reader or manually input. Recording name, document number and nationality as a minimum. Records the user that logged the entry and the location.
 - 3.3.7 Data retention period is to be a minimum of 5 years unless elsewhere agreed by the Authority.
 - 3.3.8 Back office function where enhanced users can access further detail, including searching arrivals and producing statistical reports. Data must be able to provide yearly statistics.
 - 3.3.9 Able to process large number of searches, approximately a new scan of passport/ID every 5-10 seconds, per machine.
 - 3.3.10 Ability for officers to record notes on entries
 - 3.3.11 The three passport scanning locations to continue checking watchlist data independently should a network failure occur.
 - 3.3.12 Able to record whether the system is processing inbound or outbound.
 - 3.3.13 Ability to record the scanner location for any check.
 - 3.3.14 Security features to prevent malicious interference.
 - 3.3.15 Fully networked solution. Data can be sent to all passport scanning locations from main control room. Data captured at each location accessible at other nodes.
 - 3.3.16 Is interoperable and can import data from multiple sources.
 - 3.3.17 Minimum of one hundred (100) unique user accounts at any one time. The Authority will have the rights to create/delete/amend accounts and set access rights according to their profile.
 - 3.3.18 Software required for the passport scanning solution to be security protected, e.g. non-essential USB locked, non-essential apps and software disabled.
- 3.4** The following provides the statement of requirements for the service and support:
- 3.4.1 24/7 telephone & online support
 - 3.4.2 Annual software maintenance
 - 3.4.3 Through-life Support for faults and repairs, including software/security patches in order to maintain minimum operational outputs at each location.
 - 3.4.4 On island Train the Trainer package for 10-20 enhanced users which will allow them to deliver in house initial and refresher training to

colleagues. Alternative training methodologies will be considered where on-island training is not possible/appropriate.

- 3.5** The following provides the statement of requirements for the additional items:
- 3.5.1 Security locks on all hardware in order to secure the items to a workstation
 - 3.5.2 Secure server cabinets (if required)
 - 3.5.3 Software updates
 - 3.5.4 Commercial delivery to Cyprus Airport of Arrival (APOA) or Seaport of Arrival (SPOA). Acceptable locations are:
 - 3.5.4.1 APOA: Paphos and Larnaca
 - 3.5.4.2 SPOA: Limassol New Port