



United Kingdom  
Security Vetting

## **Call-Off Order**

Multi Discipline Professional Services  
Ref: UKSV2023-002

**a call-off in relation to  
Lot 3 Management Consultancy Framework Three (MCF3)**

## RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

### Order Form

CALL-OFF REFERENCE: UKSV2023-002

THE BUYER: **Cabinet Office - UKSV**

BUYER ADDRESS 70 Whitehall, Room 140, 1st Floor, London,  
UK, SW1A 2AS

THE SUPPLIER: Baringa Partners LLP

SUPPLIER ADDRESS: 62 Buckingham Gate, London, SE1W 6AJ

REGISTRATION NUMBER: OC303471

DUNS NUMBER: 733291509

SID4GOV ID: 

### Applicable framework contract

This Order Form is for the provision of the Call-Off Deliverables and dated **7th March 2023**.

It's issued under the Framework Contract with the reference number RM6187 for the provision of Multi Discipline Professional Services.

### CALL-OFF LOT(S):

Lot 3: Complex and Transformation

### Call-off incorporated terms

The following documents are incorporated into this Call-Off Contract.

Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187

3. The following Schedules in equal order of precedence:

**Joint Schedules for RM6187 Management Consultancy Framework Three**

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors) – NOT USED
- Joint Schedule 7 (Financial Difficulties)- NOT USED
- Joint Schedule 8 (Guarantee) – NOT USED
- Joint Schedule 9 (Minimum Standards of Reliability) NOT USED
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

**Call-Off Schedules**

- Call-Off Schedule 1 (Transparency Reports) - NOT USED
- Call-Off Schedule 3 (Continuous Improvement)
- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 6 (ICT Services) – NOT USED
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)  
NOT USED
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management) – NOT USED
- Call-Off Schedule 12 (Clustering) – NOT USED
- Call-Off Schedule 13 (Implementation Plan and Testing) – NOT  
USED
- Call-Off Schedule 14 (Service Levels)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 16 (Benchmarking) – NOT USED
- Call-Off Schedule 17 (MOD Terms) – NOT USED
- Call-Off Schedule 18 (Background Checks) – NOT USED
- Call-Off Schedule 19 (Scottish Law) – NOT USED
- Call-Off Schedule 20 (Call-Off Specification) TBC POST BID
- Call-Off Schedule 21 (Northern Ireland Law) – NOT USED
- Call-Off Schedule 23 (HMRC Terms) – NOT USED

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility) - Mandatory
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

Supplier terms are not part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

## **Call-off special terms**

None

**Call-off start date:** 7<sup>th</sup> March 2023

**Call-off expiry date:** 6<sup>th</sup> September 2023

**Call-off initial period:** 6 months

**Call-off Optional Extension period:** Potential extension for additional period up to 6 months, subject to financial and internal approvals and supplier acceptance.

### **Call-off deliverables:**

See details in Call-Off Schedule 20 (Call-Off Specification)

### **Security**

Short form security requirements apply and  
Security Policy as provided at Appendix 1

### **Maximum liability**

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first contract year are:  
**£1,150,000. (one million, one hundred and fifty thousand pounds).**

### **Call-off charges**

See details in Call-Off Schedule 5 (Pricing Details)

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law
- Benchmarking using Call-Off Schedule 16 (Benchmarking)

### **Reimbursable expenses**

Recoverable as stated in Framework Schedule 3 (Framework Prices) paragraph 4.

**Payment method**

Payment will be by BACS

**Buyer's invoice address**

[REDACTED]  
Cc: [REDACTED]

Address:

[REDACTED]  
[REDACTED]  
Tel: [REDACTED]

**FINANCIAL TRANSPARENCY OBJECTIVES**

The Financial Transparency Objectives do not apply to this Call-Off Contract.

**Buyer's authorised representative**

Contact: [REDACTED]

Email: [REDACTED]

Cabinet Office, 70 Whitehall, London, SW1A 2 AS

**Buyer's security policy**

Appended at Call-Off Appendix 1

**Supplier's authorised representative**

[REDACTED]  
[REDACTED]  
[REDACTED]

**Supplier's contract manager**

[REDACTED]  
[REDACTED]  
[REDACTED]

**Progress report frequency**

Weekly one hour meeting to be attended by the Suppliers most senior nominated resource named in the Pricing Table and the Buyers nominated Programme Director.

**Progress meeting frequency**

Weekly one hour meeting to be attended by the Suppliers most senior nominated

resource named in the Pricing Table and the Buyers nominated Programme Director.

**Key staff**



**Key subcontractor(s)**

Not applicable

**Commercially sensitive information**

In accordance with Government policy, we are obliged to publish procured contracts, subject to the withholding of commercially confidential and security sensitive information by redactions.

[Supplier to append Supplier's Blue Copy Contract confirming Personal, Commercially Confidential and Security sensitive Information.]

**Service credits**

Not applicable

**Additional insurances**

Not applicable

**Guarantee**

Not applicable

**Buyer's environmental and social value policy**

Appended at Call-Off Appendix 2

**Social value commitment**

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender).

### **Formation of call off contract**

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

#### **For and on behalf of the Supplier:**

Signature: 

Name: 

Role: 

Date: 

#### **For and on behalf of the Buyer:**

Signature: 

Name: 

Role: 

Date: 

## Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
- 1.3.1 the singular includes the plural and vice versa;
  - 1.3.2 reference to a gender includes the other gender and the neuter;
  - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;
  - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
  - 1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
  - 1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
  - 1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;
  - 1.3.8 references to "**Clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these



references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.3.13 any reference in a Contract which immediately before Exit Day is a reference to (as it has effect from time to time):

(a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (**"EU References"**) which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.14 unless otherwise provided, references to **"Buyer"** shall be construed as including Exempt Buyers; and

1.3.15 unless otherwise provided, references to **"Call-Off Contract"** and **"Contract"** shall be construed as including Exempt Call-off Contracts.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

<b>"Achieve"</b>	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and <b>"Achieved"</b> , <b>"Achieving"</b> and <b>"Achievement"</b> shall be construed accordingly;
------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>"Additional Insurances"</b>	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
<b>"Admin Fee"</b>	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: <a href="http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees">http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees</a> ;
<b>"Affected Party"</b>	the Party seeking to claim relief in respect of a Force Majeure Event;
<b>"Affiliates"</b>	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
<b>"Annex"</b>	extra information which supports a Schedule;
<b>"Approval"</b>	the prior written consent of the Buyer and <b>"Approve"</b> and <b>"Approved"</b> shall be construed accordingly;

<p><b>"Audit"</b></p>	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none"> <li>a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract);</li> <li>b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Deliverables;</li> <li>c) verify the Open Book Data;</li> <li>d) verify the Supplier's and each Subcontractor's compliance with the applicable Law;</li> <li>e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;</li> <li>f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables;</li> <li>g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;</li> <li>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;</li> <li>i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts;</li> <li>j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and</li> </ul>
-----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>effectiveness with which the Relevant Authority has used its resources;</p> <p>k) verify the accuracy and completeness of any:</p> <p>(i) Management Information delivered or required by the Framework Contract; or</p> <p>(ii) Financial Report and compliance with Financial Transparency Objectives as specified by the Buyer in the Order Form;</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>"Auditor"</b>	<ul style="list-style-type: none"> <li>a) the Buyer's internal and external auditors;</li> <li>b) the Buyer's statutory or regulatory auditors;</li> <li>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</li> <li>d) HM Treasury or the Cabinet Office;</li> <li>e) any party formally appointed by the Buyer to carry out audit or similar review functions; and</li> <li>f) successors or assigns of any of the above;</li> </ul>
<b>"Authority"</b>	CCS and each Buyer;
<b>"Authority Cause"</b>	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
<b>"BACS"</b>	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
<b>"Beneficiary"</b>	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
<b>"Buyer"</b>	the relevant public sector purchaser identified as such in the Order Form;
<b>"Buyer Assets"</b>	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;

<b>"Buyer Authorised Representative"</b>	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
<b>"Buyer Premises"</b>	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
<b>"Call-Off Contract"</b>	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
<b>"Call-Off Contract Period"</b>	the Contract Period in respect of the Call-Off Contract;
<b>"Call-Off Expiry Date"</b>	the scheduled date of the end of a Call-Off Contract as stated in the Order Form;
<b>"Call-Off Incorporated Terms"</b>	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
<b>"Call-Off Initial Period"</b>	the Initial Period of a Call-Off Contract specified in the Order Form;
<b>"Call-Off Optional Extension Period"</b>	such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form;
<b>"Call-Off Procedure"</b>	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure);
<b>"Call-Off Special Terms"</b>	any additional terms and conditions specified in the Order

	Form incorporated into the applicable Call-Off Contract;
<b>"Call-Off Start Date"</b>	the date of start of a Call-Off Contract as stated in the Order Form;
<b>"Call-Off Tender"</b>	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
<b>"CCS"</b>	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
<b>"CCS Authorised Representative"</b>	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
<b>"Central Government Body"</b>	<p>a body listed in one of the following subcategories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none"> <li>a) Government Department;</li> <li>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</li> <li>c) Non-Ministerial Department; or</li> <li>d) Executive Agency;</li> </ul>
<b>"Change in Law"</b>	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;

<b>"Change of Control"</b>	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
<b>"Charges"</b>	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
<b>"Claim"</b>	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
<b>"Commercially Sensitive Information"</b>	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
<b>"Comparable Supply"</b>	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
<b>"Compliance Officer"</b>	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
<b>"Confidential Information"</b>	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as <b>"confidential"</b> ) or which ought reasonably to be considered to be confidential;



<b>"Conflict of Interest"</b>	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
<b>"Contract"</b>	either the Framework Contract or the Call-Off Contract, as the context requires;
<b>"Contract Period"</b>	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the:  a) applicable Start Date; or  b) the Effective Date  up to and including the applicable End Date;
<b>"Contract Value"</b>	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
<b>"Contract Year"</b>	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
<b>"Control"</b>	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and <b>"Controlled"</b> shall be construed accordingly;
<b>"Controller"</b>	has the meaning given to it in the GDPR;
<b>"Core Terms"</b>	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;

<p><b>"Costs"</b></p>	<p>the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:</p> <ul style="list-style-type: none"> <li>e) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including: <ul style="list-style-type: none"> <li>i) base salary paid to the Supplier Staff;</li> <li>ii) employer's National Insurance contributions;</li> <li>iii) pension contributions;</li> <li>iv) car allowances;</li> <li>v) any other contractual employment benefits;</li> <li>vi) staff training;</li> <li>vii) workplace accommodation;</li> <li>viii) workplace IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and</li> <li>ix) reasonable recruitment costs, as agreed with the Buyer;</li> </ul> </li> <li>f) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</li> <li>g) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and</li> <li>h) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</li> </ul> <p>but excluding:</p>
-----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"><li>i) Overhead;</li><li>j) financing or similar costs;</li><li>k) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;</li><li>l) taxation;</li><li>m) fines and penalties;</li><li>n) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and</li><li>o) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</li></ul> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

<b>"CRTPA"</b>	the Contract Rights of Third Parties Act 1999;
<b>"Data Protection Impact Assessment"</b>	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
<b>"Data Protection Legislation"</b>	the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy;
<b>"Data Protection Liability Cap"</b>	the amount specified in the Framework Award Form;
<b>"Data Protection Officer"</b>	has the meaning given to it in the GDPR;
<b>"Data Subject"</b>	has the meaning given to it in the GDPR;
<b>"Data Subject Access Request"</b>	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
<b>"Deductions"</b>	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
<b>"Default"</b>	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;

<b>"Default Management Charge"</b>	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
<b>"Delay Payments"</b>	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
<b>"Deliverables"</b>	Goods and/or Services that may be ordered under the Contract including the Documentation;
<b>"Delivery"</b>	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. <b>"Deliver"</b> and <b>"Delivered"</b> shall be construed accordingly;
<b>"Disclosing Party"</b>	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
<b>"Dispute"</b>	any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
<b>"Dispute Resolution Procedure"</b>	the dispute resolution procedure set out in Clause 34 (Resolving disputes);

<b>"Documentation"</b>	<p>descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:</p> <ul style="list-style-type: none"> <li>a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables</li> <li>b) is required by the Supplier in order to provide the Deliverables; and/or</li> <li>c) has been or shall be generated for the purpose of providing the Deliverables;</li> </ul>
<b>"DOTAS"</b>	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
<b>"DPA 2018"</b>	the Data Protection Act 2018;
<b>"Due Diligence Information"</b>	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
<b>"Effective Date"</b>	the date on which the final Party has signed the Contract;
<b>"EIR"</b>	the Environmental Information Regulations 2004;

<b>"Electronic Invoice"</b>	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
<b>"Employment Regulations"</b>	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
<b>"End Date"</b>	the earlier of:  a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or  b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
<b>"Environmental Policy"</b>	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
<b>"Equality and Human Rights Commission"</b>	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
<b>"Estimated Year 1 Charges"</b>	the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;

<p><b>"Estimated Yearly Charges"</b></p>	<p>means for the purposes of calculating each Party's annual liability under clause 11.2:</p> <p>i) in the first Contract Year, the Estimated Year 1 Charges; or</p> <p>ii) in any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or</p> <p>iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;</p>
<p><b>"Exempt Buyer"</b></p>	<p>a public sector purchaser that is:</p> <p>a) eligible to use the Framework Contract; and</p> <p>b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:</p> <p>i) the Regulations;</p> <p>ii) the Concession Contracts Regulations 2016 (SI 2016/273);</p> <p>iii) the Utilities Contracts Regulations 2016 (SI 2016/274);</p> <p>iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848);</p> <p>v) the Remedies Directive (2007/66/EC);</p> <p>vi) Directive 2014/23/EU of the European Parliament and Council;</p> <p>vii) Directive 2014/24/EU of the European Parliament and Council;</p> <p>viii) Directive 2014/25/EU of the European Parliament and Council; or</p> <p>ix) Directive 2009/81/EC of the European Parliament and Council;</p>



<b>“Exempt Call-off Contract”</b>	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
<b>“Exempt Procurement Amendments”</b>	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;

<b>"Existing IPR"</b>	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
<b>“Exit Day”</b>	shall have the meaning in the European Union (Withdrawal) Act 2018;
<b>"Expiry Date"</b>	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
<b>"Extension Period"</b>	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;

<p><b>“Financial Reports”</b></p>	<p>a report by the Supplier to the Buyer that:</p> <ul style="list-style-type: none"> <li>(a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier;</li> <li>(b) provides detail a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer);</li> <li>(c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and</li> <li>(d) is certified by the Supplier’s Chief Financial Officer or Director of Finance;</li> </ul>
<p><b>“Financial Representative”</b></p>	<p>a reasonably skilled and experienced member of the Supplier Staff who has specific responsibility for preparing, maintaining, facilitating access to, discussing and explaining the records and accounts of everything to do with the Contract (as referred to in Clause 6), Financial Reports and Open Book Data;</p>

<p><b>“Financial Transparency Objectives”</b></p>	<ul style="list-style-type: none"> <li>(a) the Buyer having a clear analysis of the Costs, Overhead recoveries (where relevant), time spent by Supplier Staff in providing the Services and Supplier Profit Margin so that it can understand any payment sought by the Supplier;</li> <li>(b) the Parties being able to understand Costs forecasts and to have confidence that these are based on justifiable numbers and appropriate forecasting techniques;</li> <li>(c) the Parties being able to understand the quantitative impact of any Variations that affect ongoing Costs and identifying how these could be mitigated and/or reflected in the Charges;</li> <li>(d) the Parties being able to review, address issues with and re-forecast progress in relation to the provision of the Services;</li> <li>(e) the Parties challenging each other with ideas for efficiency and improvements; and</li> <li>(f) enabling the Buyer to demonstrate that it is achieving value for money for the taxpayer relative to current market prices;</li> </ul>
<p><b>"FOIA"</b></p>	<p>the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;</p>

<b>"Force Majeure Event"</b>	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by the Affected Party, including:</p> <ul style="list-style-type: none"> <li>a) riots, civil commotion, war or armed conflict;</li> <li>b) acts of terrorism;</li> <li>c) acts of a Central Government Body, local government or regulatory bodies;</li> <li>d) fire, flood, storm or earthquake or other natural disaster,</li> </ul> <p>but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;</p>
<b>"Force Majeure Notice"</b>	<p>a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;</p>
<b>"Framework Award Form"</b>	<p>the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;</p>
<b>"Framework Contract"</b>	<p>the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;</p>
<b>"Framework Contract Period"</b>	<p>the period from the Framework Start Date until the End Date of the Framework Contract;</p>

<b>"Framework Expiry Date"</b>	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
<b>"Framework Incorporated Terms"</b>	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
<b>"Framework Optional Extension Period"</b>	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
<b>"Framework Price(s)"</b>	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
<b>"Framework Special Terms"</b>	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
<b>"Framework Start Date"</b>	the date of start of the Framework Contract as stated in the Framework Award Form;
<b>"Framework Tender Response"</b>	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
<b>"Further Competition Procedure"</b>	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
<b>"GDPR"</b>	the General Data Protection Regulation (Regulation (EU) 2016/679);
<b>"General Anti-Abuse Rule"</b>	<p>e) the legislation in Part 5 of the Finance Act 2013 and; and</p> <p>f) any future legislation introduced into parliament to counteract tax advantages arising from abusive</p>

	arrangements to avoid National Insurance contributions;
<b>"General Change in Law"</b>	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
<b>"Goods"</b>	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ;
<b>"Good Industry Practice"</b>	standards, practises, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
<b>"Government"</b>	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
<b>"Government Data"</b>	<p>the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:</p> <ul style="list-style-type: none"> <li>i) are supplied to the Supplier by or on behalf of the Authority; or</li> <li>ii) the Supplier is required to generate, process,</li> </ul>

	store or transmit pursuant to a Contract;
<b>"Guarantor"</b>	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
<b>"Halifax Abuse Principle"</b>	the principle explained in the CJEU Case C-255/02 Halifax and others;
<b>"HMRC"</b>	Her Majesty's Revenue and Customs;
<b>"ICT Policy"</b>	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;

<b>"Impact Assessment"</b>	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> <li>a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;</li> <li>b) details of the cost of implementing the proposed Variation;</li> <li>c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practises of either Party;</li> <li>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and</li> <li>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;</li> </ul>
<b>"Implementation Plan"</b>	<p>the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;</p>
<b>"Indemnifier"</b>	<p>a Party from whom an indemnity is sought under this Contract;</p>
<b>"Independent Control"</b>	<p>where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and <b>"Independent Controller"</b> shall be construed accordingly;</p>



<b>"Indexation"</b>	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
<b>"Information"</b>	has the meaning given under section 84 of the Freedom of Information Act 2000;
<b>"Information Commissioner"</b>	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
<b>"Initial Period"</b>	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;

<p><b>"Insolvency Event"</b></p>	<p>with respect to any person, means:</p> <p>(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:</p> <p>(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or</p> <p>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;</p> <p>(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;</p> <p>(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days;</p> <p>(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;</p> <p>(f) where that person is a company, a LLP or a partnership:</p> <p>(i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up</p>
----------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;</p> <p>(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or</p> <p>(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or</p> <p>(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>"Installation Works"</b>	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
<b>"Intellectual Property Rights" or "IPR"</b>	<ul style="list-style-type: none"> <li>a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</li> <li>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and</li> <li>c) all other rights having equivalent or similar effect in any country or jurisdiction;</li> </ul>
<b>"Invoicing Address"</b>	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
<b>"IPR Claim"</b>	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
<b>"IR35"</b>	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: <a href="https://www.gov.uk/guidance/ir35-find-out-if-it-applies">https://www.gov.uk/guidance/ir35-find-out-if-it-applies</a> ;
<b>"Joint Controller Agreement"</b>	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in

	Annex 2 of Joint Schedule 11 ( <i>Processing Data</i> );
<b>"Joint Controllers"</b>	where two or more Controllers jointly determine the purposes and means of Processing;
<b>"Key Staff"</b>	the individuals (if any) identified as such in the Order Form;
<b>"Key Sub-Contract"</b>	each Sub-Contract with a Key Subcontractor;
<b>"Key Subcontractor"</b>	<p>any Subcontractor:</p> <ul style="list-style-type: none"> <li>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</li> <li>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or</li> <li>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract,</li> </ul> <p>and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;</p>
<b>"Know-How"</b>	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;

<b>"Law"</b>	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
<b>"LED"</b>	Law Enforcement Directive (Directive (EU) 2016/680);
<b>"Losses"</b>	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and <b>"Loss"</b> shall be interpreted accordingly;
<b>"Lots"</b>	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
<b>"Management Charge"</b>	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
<b>"Management Information" or "MI"</b>	the management information specified in Framework Schedule 5 (Management Charges and Information);
<b>"MI Default"</b>	means when two (2) MI Reports are not provided in any rolling six (6) month period

<b>"MI Failure"</b>	<p>means when an MI report:</p> <ul style="list-style-type: none"> <li>a) contains any material errors or material omissions or a missing mandatory field; or</li> <li>b) is submitted using an incorrect MI reporting Template; or</li> <li>c) is not submitted by the reporting date (including where a declaration of no business should have been filed);</li> </ul>
<b>"MI Report"</b>	<p>means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);</p>
<b>"MI Reporting Template"</b>	<p>means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;</p>
<b>"Milestone"</b>	<p>an event or task described in the Implementation Plan;</p>
<b>"Milestone Date"</b>	<p>the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;</p>
<b>"Month"</b>	<p>a calendar month and <b>"Monthly"</b> shall be interpreted accordingly;</p>
<b>"National Insurance"</b>	<p>contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);</p>

<p><b>"New IPR"</b></p>	<p>IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or</p> <p>IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same;</p> <p>but shall not include the Supplier's Existing IPR;</p>
<p><b>"Occasion of Tax Non-Compliance"</b></p>	<p>where:</p> <ul style="list-style-type: none"> <li>a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: <ul style="list-style-type: none"> <li>i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;</li> <li>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or</li> </ul> </li> <li>b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;</li> </ul>



<p><b>"Open Book Data "</b></p>	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:</p> <ul style="list-style-type: none"> <li>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;</li> <li>b) operating expenditure relating to the provision of the Deliverables including an analysis showing: <ul style="list-style-type: none"> <li>iii) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;</li> <li>iv) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade;</li> <li>v) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and</li> <li>vi) Reimbursable Expenses, if allowed under the Order Form;</li> </ul> </li> <li>c) Overheads;</li> <li>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</li> <li>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</li> <li>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;</li> <li>g) an explanation of the type and value of risk and contingencies associated with the provision of the</li> </ul>
---------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Deliverables, including the amount of money attributed to each risk and/or contingency; and</p> <p>h) the actual Costs profile for each Service Period;</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>"Order"</b>	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
<b>"Order Form"</b>	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
<b>"Order Form Template"</b>	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);
<b>"Other Contracting Authority"</b>	any actual or potential Buyer under the Framework Contract;
<b>"Overhead"</b>	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
<b>"Parliament"</b>	takes its natural meaning as interpreted by Law;
<b>"Party"</b>	in the context of the Framework Contract, CCS or the Supplier, and in the context of a Call-Off Contract the Buyer or the Supplier. <b>"Parties"</b> shall mean both of them where the context permits;
<b>"Performance Indicators" or "PIs"</b>	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
<b>"Personal Data"</b>	has the meaning given to it in the GDPR;

<b>“Personal Data Breach”</b>	has the meaning given to it in the GDPR;
<b>“Personnel”</b>	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
<b>"Prescribed Person"</b>	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: <a href="https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies">https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies</a> ;
<b>“Processing”</b>	has the meaning given to it in the GDPR;
<b>“Processor”</b>	has the meaning given to it in the GDPR;
<b>“Processor Personnel”</b>	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
<b>"Progress Meeting"</b>	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
<b>"Progress Meeting Frequency"</b>	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
<b>“Progress Report”</b>	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;

<b>“Progress Report Frequency”</b>	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
<b>“Prohibited Acts”</b>	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <p>vii) induce that person to perform improperly a relevant function or activity; or</p> <p>viii) reward that person for improper performance of a relevant function or activity;</p> <p>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or</p> <p>c) committing any offence:</p> <p>ix) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or</p> <p>x) under legislation or common law concerning fraudulent acts; or</p> <p>xi) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or</p> <p>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;</p>

<b>“Protective Measures”</b>	appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
<b>“Recall”</b>	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
<b>"Recipient Party"</b>	the Party which receives or obtains directly or indirectly Confidential Information;
<b>"Rectification Plan"</b>	<ul style="list-style-type: none"> <li>a) the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:</li> <li>b) full details of the Default that has occurred, including a root cause analysis;</li> <li>c) the actual or anticipated effect of the Default; and</li> <li>d) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);</li> </ul>
<b>"Rectification Plan Process"</b>	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);

<b>"Regulations"</b>	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
<b>"Reimbursable Expenses"</b>	<p>the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:</p> <ul style="list-style-type: none"> <li>a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agreed in advance in writing; and</li> <li>b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;</li> </ul>
<b>"Relevant Authority"</b>	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
<b>"Relevant Authority's Confidential Information"</b>	<ul style="list-style-type: none"> <li>a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);</li> <li>b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and</li> </ul>

	information derived from any of the above;
<b>"Relevant Requirements"</b>	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
<b>"Relevant Tax Authority"</b>	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
<b>"Reminder Notice"</b>	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;
<b>"Replacement Deliverables"</b>	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
<b>"Replacement Subcontractor"</b>	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);



<b>"Replacement Supplier"</b>	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
<b>"Request For Information"</b>	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
<b>"Required Insurances"</b>	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
<b>"Satisfaction Certificate"</b>	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
<b>"Security Management Plan"</b>	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
<b>"Security Policy"</b>	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
<b>"Self Audit Certificate"</b>	means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
<b>"Serious Fraud Office"</b>	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

<b>"Service Levels"</b>	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
<b>"Service Period"</b>	has the meaning given to it in the Order Form;
<b>"Services"</b>	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
<b>"Service Transfer"</b>	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
<b>"Service Transfer Date"</b>	the date of a Service Transfer;
<b>"Sites"</b>	<p>any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:</p> <ul style="list-style-type: none"> <li>a) the Deliverables are (or are to be) provided; or</li> <li>b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;</li> <li>c) those premises at which any Supplier Equipment or any part of the Supplier System is located (where any part of the Deliverables provided falls within Call-Off Schedule 6 (ICT Services));</li> </ul>
<b>"SME"</b>	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;

<b>"Special Terms"</b>	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
<b>"Specific Change in Law"</b>	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
<b>"Specification"</b>	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;
<b>"Standards"</b>	<p>any:</p> <ul style="list-style-type: none"> <li>a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with;</li> <li>b) standards detailed in the specification in Schedule 1 (Specification);</li> <li>c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;</li> <li>d) relevant Government codes of practice and guidance applicable from time to time;</li> </ul>
<b>"Start Date"</b>	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;

<b>"Statement of Requirements"</b>	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
<b>"Storage Media"</b>	the part of any device that is capable of storing and retrieving data;
<b>"Sub-Contract"</b>	<p>any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party:</p> <ul style="list-style-type: none"> <li>a) provides the Deliverables (or any part of them);</li> <li>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or</li> <li>c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);</li> </ul>
<b>"Subcontractor"</b>	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
<b>"Subprocessor"</b>	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
<b>"Supplier"</b>	the person, firm or company identified in the Framework Award Form;
<b>"Supplier Assets"</b>	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
<b>"Supplier Authorised Representative"</b>	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;

<b>"Supplier's Confidential Information"</b>	<ul style="list-style-type: none"> <li>a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;</li> <li>b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract;</li> <li>c) Information derived from any of (a) and (b) above;</li> </ul>
<b>"Supplier's Contract Manager"</b>	<p>the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;</p>
<b>"Supplier Equipment"</b>	<p>the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;</p>
<b>"Supplier Marketing Contact"</b>	<p>shall be the person identified in the Framework Award Form;</p>
<b>"Supplier Non-Performance"</b>	<p>where the Supplier has failed to:</p> <ul style="list-style-type: none"> <li>a) Achieve a Milestone by its Milestone Date;</li> <li>b) provide the Goods and/or Services in accordance with the Service Levels ; and/or</li> <li>c) comply with an obligation under a Contract;</li> </ul>

<b>"Supplier Profit"</b>	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
<b>"Supplier Profit Margin"</b>	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
<b>"Supplier Staff"</b>	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
<b>"Supporting Documentation"</b>	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;
<b>"Termination Notice"</b>	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
<b>"Test Issue"</b>	any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract;
<b>"Test Plan"</b>	a plan: <ul style="list-style-type: none"> <li>a) for the Testing of the Deliverables; and</li> <li>b) setting out other agreed criteria related to the achievement of Milestones;</li> </ul>

<b>"Tests "</b>	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and <b>"Tested"</b> and <b>"Testing"</b> shall be construed accordingly;
<b>"Third Party IPR"</b>	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
<b>"Transferring Supplier Employees"</b>	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
<b>"Transparency Information"</b>	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – <ul style="list-style-type: none"> <li>(i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and</li> <li>(ii) Commercially Sensitive Information;</li> </ul>
<b>"Transparency Reports"</b>	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
<b>"Variation"</b>	any change to a Contract;
<b>"Variation Form"</b>	the form set out in Joint Schedule 2 (Variation Form);
<b>"Variation Procedure"</b>	the procedure set out in Clause 24 (Changing the contract);

<b>"VAT"</b>	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
<b>"VCSE"</b>	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
<b>"Worker"</b>	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) ( <a href="https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees">https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees</a> ) applies in respect of the Deliverables;
<b>"Working Day"</b>	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;
<b>"Work Day"</b>	8.0 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
<b>"Work Hours"</b>	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.



## Joint Schedule 2 (Example Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details	
This variation is between:	<p><b>[delete as applicable: CCS / Buyer] ("CCS" "the Buyer")</b></p> <p>And</p> <p><b>[insert name of Supplier] ("the Supplier")</b></p>
Contract name:	<b>[insert name of contract to be changed] ("the Contract")</b>
Contract reference number:	<b>[insert contract reference number]</b>
Details of Proposed Variation	
Variation initiated by:	<b>[delete as applicable: CCS/Buyer/Supplier]</b>
Variation number:	<b>[insert variation number]</b>
Date variation is raised:	<b>[insert date]</b>
Proposed variation	
Reason for the variation:	<b>[insert reason]</b>

An Impact Assessment shall be provided within:	<b>[insert number]</b> days	
<b>Impact of Variation</b>		
Likely impact of the proposed variation:	<b>[Supplier to insert assessment of impact]</b>	
<b>Outcome of Variation</b>		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> <li>• <b>[CCS/Buyer to insert original Clauses or Paragraphs to be varied and the changed clause]</b></li> </ul>	
Financial variation:	Original Contract Value:	£ <b>[insert amount]</b>
	Additional cost due to variation:	£ <b>[insert amount]</b>
	New Contract value:	£ <b>[insert amount]</b>

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete as applicable: CCS / Buyer]**
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete as applicable: CCS / Buyer]**

Signature	
Date	
Name (in Capitals)	
Address	

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature	
Date	
Name (in Capitals)	
Address	

# Joint Schedule 3 (Insurance Requirements)

## 1. The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

## 2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 Hold all policies in respect of the Insurances and cause any insurance broker affecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

### **3. What happens if you aren't insured**

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

### **4. Evidence of insurance you must provide**

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

### **5. Making sure you are insured to the required amount**

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

### **6. Cancelled Insurance**

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant

Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

## **7. Insurance claims**

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall cooperate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.
- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

## **ANNEX: REQUIRED INSURANCES**

**1.** The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:

- 1.1 professional indemnity insurance with cover (for a single claim or a series of related claims and in the aggregate) of not less than five million pounds (£5,000,000);
- 1.2 public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and
- 1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

## Joint Schedule 4 (Commercially Sensitive Information)

### 1. What is Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

	Date	Item(s)	Duration of Confidentiality
	1 March 2023	Supplier's pricing model and day rates	5 years



## Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan		
Details of the Default:	[ <b>Guidance:</b> Explain the Default, with clear schedule and clause references as appropriate]	
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 7 days from request)]	
Signed by [CCS/Buyer] :		Date:
Supplier [Revised] Rectification Plan		
Cause of the Default	[add cause]	
Anticipated impact assessment:	[add impact]	
Actual effect of Default:	[add effect]	
Steps to be taken to rectification:	<b>Steps</b>	<b>Timescale</b>
	1.	[date]
	2.	[date]

	3.	[date]	
	4.	[date]	
	[...]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	<b>Steps</b>	<b>Timescale</b>	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[...]	[date]	
Signed by the Supplier:		Date:	
<b>Review of Rectification Plan [CCS/Buyer]</b>			

Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[add reasons]		
Signed by [CCS/Buyer]		Date:	

# Joint Schedule 11 (Processing Data)

## Definitions

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

<b>“Processor Personnel”</b>	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:
  - (a) “Controller” in respect of the other Party who is “Processor”;
  - (b) “Processor” in respect of the other Party who is “Controller”;
  - (c) “Joint Controller” with the other Party;
  - (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

## Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.

- 5.** The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged Processing and the purpose of the Processing;
  - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 6.** The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
  - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
    - (i) nature of the data to be protected;
    - (ii) harm that might result from a Personal Data Breach;
    - (iii) state of technological development; and
    - (iv) cost of implementing any measures;
  - (c) ensure that :
    - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
    - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
      - (A) are aware of and comply with the Processor's duties

under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

- (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
  - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
  - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
  - (ii) the Data Subject has enforceable rights and effective legal remedies;
  - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 7.** Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);

- (b) receives a request to rectify, block or erase any Personal Data;
  - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
  - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
  - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
  - (f) becomes aware of a Personal Data Breach.
- 8.** The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
- 9.** Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
  - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
  - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
  - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 10.** The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
  - (b) the Controller determines the Processing includes special categories

of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

- (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

**11.** The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

**12.** The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

**13.** Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

- (a) notify the Controller in writing of the intended Subprocessor and Processing;
- (b) obtain the written consent of the Controller;
- (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
- (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

**14.** The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

**15.** The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

**16.** The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

#### **Where the Parties are Joint Controllers of Personal Data**

**17.** In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set



out in Annex 2 to this Joint Schedule 11.

### **Independent Controllers of Personal Data**

- 18.** With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
- 19.** Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
- 20.** Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
- 21.** The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
- 22.** The Parties shall only provide Personal Data to each other:

  - (a) to the extent necessary to perform their respective obligations under the Contract;
  - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
  - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
- 23.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection

Legislation, including Article 32 of the UK GDPR.

- 24.** A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
- 25.** Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
  - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
    - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
    - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 26.** Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
  - (b) implement any measures necessary to restore the security of any compromised Personal Data;
  - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

- (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 27.** Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 28.** Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 29.** Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are:  
dpo@cabinetoffice.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are:

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Relevant Authority is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Duration of the Processing	<p>Access to the data shall coincide with the duration of the contract only [REDACTED] unless otherwise extended by agreement of the Parties.</p>

Nature and purposes of the Processing	Names and contact details will be used to progress the delivery of the Multi Discipline Professional Services contract as daily contact points. The nature of the services will not involve access to or the recording/storage of personal data.
Type of Personal Data	Name, official role, business email, telephone number, possible business addresses.
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers. customers/ clients and potentially associated government bodies.
Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under Union or Member State law to preserve that type of data	<div style="background-color: black; width: 100%; height: 100px; margin-bottom: 10px;"></div> <div style="background-color: black; width: 100%; height: 60px; margin-bottom: 10px;"></div> <div style="background-color: black; width: 100%; height: 40px; margin-bottom: 10px;"></div> <div style="background-color: black; width: 100%; height: 80px;"></div>

## **Annex 2 - Joint Controller Agreement NOT USED**

### **1. Joint Controller Status and Allocation of Responsibilities**

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection

Legislation as against the relevant Party as Controller.

## **2. Undertakings of both Parties**

1.1.2.1 The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every [x] months on:
  - (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
  - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
  - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
  - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
  - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third

party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
  - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
  - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
  - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Personal Data Breach;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or



correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

- (j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

1.1.2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

### **3. Data Protection Breach**

1.1.3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
  - (i) cooperation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
  - (ii) cooperation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
  - (iii) coordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
  - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach,

with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

1.1.3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

#### **4. Audit**

1.1.4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

1.1.4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

## **5. Impact Assessments**

1.1.5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

## **6. ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

## **7. Liabilities for Data Protection Breach**

**[Guidance:** This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

1.1.7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its

reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree to such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

1.1.7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

1.1.7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the

Claim Losses equally.

1.1.7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

## **8. Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

## **9. Sub-Processing**

1.1.9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

## **10. Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

## 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 (1<sup>st</sup>) 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 (1<sup>st</sup>) 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 5 (Pricing Details)

1.1 The Supplier shall provide the services based on capped time and materials for the resourcing and day rates confirmed below.

1.2

1.3 [REDACTED]

[illegible]

**Notes to the Pricing:**

Prices shown exclude VAT.

Pricing is inclusive of all expenses.

The currency is British pounds sterling (GBP), no decimal places.

Pricing is based on an eight (8) hour Working Day

Payments will be monthly in arrears upon performance of the services in accordance with their descriptions in this Call Off Contract/progress which shall be agreed at monthly meetings

## Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

- 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
- 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
- 1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

- 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
- 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
- 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least

three (3) Months' notice;

- 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
  - 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

## Call-Off Schedule 9 (Security Short)

### 1. Definitions

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

<b>"Breach of Security"</b>	<p>1 the occurrence of:</p> <ul style="list-style-type: none"><li>a) any unauthorised access to or use of the 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</li><li>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,</li></ul> <p>2 in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;</p>
<b>"Security Management Plan"</b>	<p>3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and has been updated from time to time.</p>

## **2. Complying with security requirements and updates to them**

- 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 Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.3** Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.4** If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables, it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
- 2.5** Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

## **3. Security Standards**

- 3.1** 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 security.
- 3.2** The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
  - 3.2.1** is in accordance with the Law and this Contract;
  - 3.2.2** as a minimum demonstrates Good Industry Practice;
  - 3.2.3** meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
  - 3.2.4** where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
- 3.3** The references to standards, guidance and policies contained or set out in Paragraph 3.2 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.

- 3.4** In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

## **4. Security Management Plan**

### **4.1 Introduction**

- 4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

### **4.2 Content of the Security Management Plan**

- 4.2.1 The Security Management Plan shall:

- a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
- b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites 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;
- d) 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, 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;
- e) 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 provision of the Goods and/or Services and shall 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 Contract;

- f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

#### **4.3 Development of the Security Management Plan**

- 4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
- 4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will 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 its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
- 4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer



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.

- 4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

#### **4.4 Amendment of the Security Management Plan**

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

- a) emerging changes in Good Industry Practice;
- b) any change or proposed change to the Deliverables and/or associated processes;
- c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;
- d) any new perceived or changed security threats; and
- e) any reasonable change in requirements requested by the Buyer.

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

- a) suggested improvements to the effectiveness of the Security Management Plan;
- b) updates to the risk assessments; and
- c) suggested improvements in measuring the effectiveness of controls.

- 4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

- 4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the 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.

## **5. Security breach**

**5.1** Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

**5.2** Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

**5.2.1** 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 to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
- c) prevent an equivalent breach in the future exploiting the same cause failure; and
- d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

**5.3** 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 Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

## Call-Off Schedule 14 (Service Levels)

### 1. Definitions

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

<b>"Critical Service Level Failure"</b>	has the meaning given to it in the Order Form;
<b>"Service Credits"</b>	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
<b>"Service Credit Cap"</b>	has the meaning given to it in the Order Form;
<b>"Service Level Failure"</b>	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
<b>"Service Level Performance Measure"</b>	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
<b>"Service Level Threshold"</b>	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

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

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service

Credit is 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.

- 2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.
- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
  - 2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
  - 2.4.2 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
  - 2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
- 2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
  - 2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
  - 2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
  - 2.5.3 there is no change to the Service Credit Cap.

### **3. Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

- 3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

## Part A: Service Levels

### 1. Service Levels

If the level of performance of the Supplier:

- 1.1 is likely to or fails to meet any Service Level Performance Measure; or
- 1.2 is likely to cause or causes a Critical Service Failure to occur,

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.a.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.a.2 instruct the Supplier to comply with the Rectification Plan Process;
- 1.a.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- 1.a.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).

## Annex A to Part A: Services Levels

No.	Key	Service Level description	Target
1	Timeliness	Commencement: Deployment of cleared resources no later than 7 <sup>th</sup> March 2023	07/03/23
2	Timeliness	Progress Updates: Weekly update to confirm progress, risks and issues which may impact upon delivery within the pillar(s)	Weekly with information to enable management of delivery on time
3	Accuracy and Quality	Output, performance and conduct: Supplier resources shall undertake their roles in a professional manner	No more than one error or complaint per 2 month rolling period in respect of delivery
4	Timeliness and Accuracy	Invoicing: Draft Invoice and supporting performance presented at monthly meeting for approval. Approved invoice submitted within a week of monthly meeting .	Draft invoice presented at monthly meeting



# Call-Off Schedule 15 (Call-Off Contract Management)

## 1. Definitions

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

<b>"Operational Board"</b>	the board established in accordance with paragraph 4.1 of this Schedule;
<b>"Project Manager"</b>	the manager appointed in accordance with paragraph 2.1 of this Schedule;

## 2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resources are made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

## 3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager'(s) shall be:

- 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;
- 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding

with the delegation and it will be delegated person's responsibility to fulfil the Supplier's Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager(s) in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager(s) by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

#### **4. Role of the Operational Board**

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.



- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

## **5. Contract Risk Management**

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
- 5.2.1 the identification and management of risks;**
  - 5.2.2 the identification and management of issues; and
  - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer and the Supplier have identified.

# **Annex: Contract Boards**

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

1. The Supplier's Lead shall meet with the Authority to provide a weekly progress report identifying actions complete, next steps and any risks or issues impacting the delivery of the report(s).
2. The Supplier shall also meet on a monthly basis to confirm consumption of resources/costs against the project plan to ensure resourcing and progress is managed appropriately and the SLA set out in Call Off Schedule 14 Annex A are being achieved.

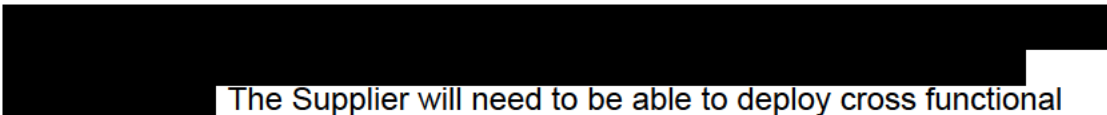
# Call-Off Schedule 20 (Call-Off Specification)

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

## OVERVIEW

- 1.1 UKSV is a business unit of the Cabinet Office and we generate our own revenues by burden-share across the secure government community and this is very much a delivery organisation.
- 1.2 UKSV transitioned from MOD to Cabinet Office in 2020. During this time, UKSV has maintained delivery of vetting services to the public and secure partners across government, whilst updating and modernising legacy systems and processes to deliver a future agile and efficient vetting service under two major programmes: Vetting Transformation Programme (VTP) and the Delivery Stabilisation Programme (DSP).

## 2. BACKGROUND

- 2.1  The Supplier will need to be able to deploy cross functional experienced teams at pace and draw on subject matter experts from a broad range of capabilities from within the organisation.
- 2.2 The focus of the Supplier teams will be on improving transparency on governance, planning, performance management and delivery to help ensure objectives are met in line with business cases.
- 2.3 Teams will be required for six months, with the Buyer reserving a right to implement an extension for up to a further six months, subject to funding provision, internal approvals and acceptance by the supplier.

## 3. THE SERVICES

- 3.1 The Supplier shall support the transformation programmes assigned to the following internal Buyer functions:
  - Programme Management
  - People, and
  - Commercial

Supplier shall work at the direction and management of the Buyer on a time and materials basis to provide the services.

### 3.2 Transformation Programme Pillar: Stabilise

- 3.2.1 Commercial – a major programme requires enhanced commercial planning and management.
- 3.2.3 Programme delivery – A governance structure is in place and requires strengthening of support to ensure the control of multiple projects and changes.
- 3.2.3 People - as the business progresses through change the journey that our employees face will be complex, challenging and rewarding, hence will require close management and engagement.

### 3.3 Transformation Programme Pillar: Enhance

- 3.3.1 Performance Review – support is required to measure current performance through a set of internal baselines (e.g. function vs. function, or pre-pandemic vs. post pandemic etc.) and to control the immediate opportunity for improvement to process and practice.
- 3.3.2 People Led Productivity – whilst the business case for a new technological solution is progressing, support is required to implement people led productivity improvements to address current backlogs.
- 3.3.3 Ops Enablement Improvement – alongside the focus on vetting service delivery processes, support is required to review and improve the processes which make vetting operations run, e.g. planning, performance and governance to improve effectiveness, transparency and control
- 3.3.4 Leadership Development – delivering the benefits from the above requires change in leadership behaviour due to the increased ownership taken by junior leaders and changes to how operational performance is managed. Delivering an empowerment focused leadership development programme ensures this change is implemented deep into the grade structure ensuring momentum for change is gained. This also supports the exit management of the professional services team.

### 3.4 Transformation Programme Pillar: Transform

- 3.4.1 Vision and Strategy – the focus of the programme to date has been plugging technology and operational gaps. The future ambitious vision needs to be transparent on how we will deliver a safe, secure, rapid and reliable vetting service, across all levels. It needs to be scalable, automated and able to deliver against all use cases with a clear benefit case.
- 3.4.2 Roadmap – a transformation roadmap to achieve the strategy needs to be set out at hi and lo detail.
- 3.4.3 Business case – a business case to deliver the Transformation vision needs to be taken through CO approvals to secure the funding to deliver the programme.
- 3.4.5 Programme delivery – programme governance needs to be aligned with the strategy, and the delivery of the business case.
- 3.4.7 Data privacy and information security – appropriate expertise is required to ensure the solution is future proofed and secure given the sensitivity of the service.

### 3.5 In addition the Supplier shall assist by addressing the following:

- 3.5.1 Ensure that there are appropriate meetings to understand the roadmap, and delivery is aligned across workstreams (this needs to include all those in leadership across the programme) (Essential)

- 3.5.2 Ensure that there is an appropriate contract management, and regular review of the outcomes and how this relates to the overall roadmap or plan (Critical)
- 3.5.3 Ensure all key agreed transformation activities are monitored.(Essential)
- 3.5.4 System integration requires a full time change team to plan and implement, but will yield efficiency gains across the Buyer's organisation (Essential)
- 3.5.4 Review all procurement requirements and specifications - making outcomes and key performance indicators clear and smart
- 3.5.5 Put a commercial strategy in place for all current and future contracts - including ones which are expiring in the near future, which will support timely finalisation of COAB business cases and approval submissions
- 3.5.6 PMO and Audit & Assurance Team's respective roles and responsibilities are clearly defined to ensure that associated resources and plans are effectively coordinated and provide optimal coverage, aligned to the delivery and risk position.
- 3.6 The Supplier Team and indicative resourcing is confirmed in the table below:

[illegible]

#### 4. BASE LOCATION

- 4.1 The location of the Services will be carried out predominantly using a hybrid of supplier's own site with some attendance at site in person when required at [REDACTED] sites.
- 4.2 The majority of meeting attendance is conducted on a remote basis.

## **5. STAFF VETTING, EXPERIENCE AND QUALIFICATIONS**

- 5.1 All resources assigned to deliver the requirement shall be security cleared. Security clearance requirements will be handled at the discretion of the Buyer on a strict needs basis and it is expected for the duration of the contract the supplier assigned resources shall hold all necessary security clearances.
- 5.2 All resources assigned, shall hold an appropriate professional qualification relevant to the discipline (i.e. APM/PRINCE2, MCIPS, CISMP etc) and have experience of operational delivery roles.

## **6. KEY MILESTONES**

- 6.1 The Supplier should note the following project milestones that the Buyer will measure the progress and quality of delivery against the following indicative milestones:

**Milestone 1:** Completion of transformation business case

**Timeframe:** July '23

**Milestone 2:** People Programme Plan

**Timeframe:** June '23

**Milestone 3:** Commercial Strategy

**Timeframe:** July '23

## **7. BUYER'S RESPONSIBILITIES**

- 7.1 The Buyer shall provide suitable team working space for the project team if required to be on premises at any of the key locations
- 7.2 The Buyer shall facilitate the process of verification/transfer of SC Clearances. Any sponsorship required to support new clearances shall be at the sole discretion of the Buyer
- 7.3 The Buyer shall make its equipment (Cabinet Office laptops), software, tools and relevant licences available to the Supplier where necessary to deliver the services.
- 7.4 The Supplier will be dependent on the Buyer to ensure that UKSV staff and information is made available in a timely fashion so that the Supplier can work at the Buyers direction to deliver the Services
- 7.5 Supplier accepts no liability for errors in Services and Deliverables provided, in reliance upon the Buyer's own provided materials and data. However, the Supplier shall be obliged to confirm any apparent mistake or error prior to expending resources.

# Call Off Appendix 1 Security

**In this Schedule Appendix 1 (Security Management):**

## 1. Definitions

“Anti-virus Software”	<p>means software that:</p> <ul style="list-style-type: none"> <li><b>a.</b> protects the Supplier Information Management System from the possible introduction of Malicious Software;</li> <li><b>b.</b> scans for and identifies possible Malicious Software in the Supplier Information Management System;</li> <li><b>c.</b> if Malicious Software is detected in the Supplier Information Management System, so far as possible: <ul style="list-style-type: none"> <li><b>i.</b> prevents the harmful effects of the Malicious Software; and</li> <li><b>ii.</b> removes the Malicious Software from the Supplier Information Management System;</li> </ul> </li> </ul>
“Breach of Security”	<p>means the occurrence of:</p> <ul style="list-style-type: none"> <li><b>a.</b> any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement;</li> <li><b>b.</b> the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or</li> <li><b>c.</b> any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;</li> </ul>
“Buyer Data”	<p><b>means any:</b></p> <ul style="list-style-type: none"> <li><b>d.</b> data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or</li> <li><b>e.</b> Personal Data for which the Buyer is a, or the, Data Controller, that is: <ul style="list-style-type: none"> <li><b>a.</b> supplied to the Supplier by or on behalf of the Buyer; or</li> <li><b>b.</b> that the Supplier generates, processes, stores or transmits under this Agreement.</li> </ul> </li> </ul>
“Buyer Equipment”	<p>means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;</p>
“Buyer System”	<p>means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services;</p>
“Certification Default”	<p><b>means the occurrence of one or more of the circumstances listed in Paragraph 6.4;</b></p>
“Certification Rectification Plan”	<p><b>means the plan referred to in Paragraph 6.5.1;</b></p>

“Certification Requirements”	<b>means the information security requirements set out in paragraph 6.</b>
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“HMG Baseline Personnel Security Standard”	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 ( <a href="https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf">https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf</a> ), as that document is updated from time to time;
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
“NCSC Cloud Security Principles”	means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at <a href="https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles">https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles</a> .
“NCSC Device Security Guidance”	means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at <a href="https://www.ncsc.gov.uk/collection/device-security-guidance">https://www.ncsc.gov.uk/collection/device-security-guidance</a> ;
“Privileged User”	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
“Process”	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
“Prohibited Activity”	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
“Prohibition Notice”	means a notice issued under paragraph 1.3 of Annex 1.



<b>“Relevant Certifications”</b>	means those certifications specified in Paragraph 6.1;
<b>“Relevant Convictions”</b>	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), offences against property, drugs, alcohol, public order offences or any other offences relevant to Services as the Buyer may specify;
<b>“Security Management Plan”</b>	means the document prepared in accordance with the requirements of Paragraph 7
<b>“Sites”</b>	means any premises: <b>a.</b> from or at which: <b>i.</b> the Services are (or are to be) provided; or <b>ii.</b> the Supplier manages, organises or otherwise directs the provision or the use of the Services; or <b>b.</b> where: <b>i.</b> any part of the Supplier Information Management System is situated; or <b>ii.</b> any physical interface with the Buyer System takes place;
<b>“Standard Contractual Clauses”</b>	means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area;
<b>“Supplier Information Management System”</b>	means: <b>a.</b> those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and <b>b.</b> the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
<b>“Sub-contractor Personnel”</b>	means: <b>a.</b> any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and <b>b.</b> engaged in or likely to be engaged in: <b>i.</b> the performance or management of the Services; <b>ii.</b> or the provision of facilities or services that are necessary for the provision of the Services.
<b>“Supplier Personnel”</b>	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement;
<b>“UKAS”</b>	means the United Kingdom Accreditation Service;

## 2. Introduction

2.1 This Schedule Appendix 1 (Security Management) sets out:

- ii. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;
- iii. the assessment of this Agreement as either a:
  - 1. Standard consultancy agreement; or
  - 2. Higher-risk consultancy agreement,  
in Paragraph 3;
- iv. the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 4;
- v. the Certification Requirements, in Paragraph 5;
- vi. the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in Paragraph 6;
- vii. the security requirements with which the Supplier must comply in Annex 1;

## 3. Principles of Security

3.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

the Sites;

the Services; and

the Supplier's Information Management System.

3.2 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors; and

3.2.2 the security of the Supplier Information Management System.

3.3 The Supplier shall:

3.3.1 comply with the security requirements in Annex 1; and

3.3.2 ensure that each Sub-contractor that Processes Buyer Data complies with the Sub-contractor security requirements in Annex 1.

- 3.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

## 4. Buyer Risk Assessment

- 4.1 The Buyer has assessed this Agreement as

- ☒ A standard consultancy
- ☐ A higher-risk consultancy agreement.

## 5. Access to Supplier Personnel and Supplier Information Management System

- 5.1 The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

access to the Supplier Personnel;

access to the Information Management System to audit the Supplier and its Sub-contractors' compliance with this Agreement; and

such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

- 5.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 5.6 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

## 6. Certification Requirements

- 6.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

1. In the case of a standard consultancy agreement:

☒ Cyber Essentials Plus;

☐ Cyber Essentials; or

- 6.2 In the case of a higher-risk consultancy agreement:

**ISO/IEC 27001:2018 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier**

**Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2018; and**

**Cyber Essentials Plus (the “Relevant Certifications”).**

- 6.3 Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.
- 6.4 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:
- Currently in effect;
  - Relate to the full scope of the Supplier Information System; and
  - Are not subject to any condition that may impact the provision of the Services.
- 6.5 The Supplier must notify the Buyer promptly, any in any event within three (3) Working Days of becoming aware that:
- A Relevant Certification has been revoked or cancelled by the body that awarded it;
  - A Relevant Certification expired and has not been renewed by the Supplier;
  - A Relevant Certification no longer applies to the full scope of the Supplier Information Management System or
  - The body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a **“Certification Default”**)
- 6.6 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 6.4:
- the Supplier must, within 10 working Days of the date in which the Supplier provided notice under Paragraph 6.4 (or such other period as the Parties may agree) provide a draft plan (a **“Certification Rectification Plan”**) to the Supplier setting out:
    - full details of the Certification Default, including a root cause analysis;**
    - the actual and anticipated effects of the Certification Default;**
    - the steps the Supplier will take to remedy the Certification Default;**
  - the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
- 6.7 If the Buyer rejects the Certification Rectification Plan, the Buyer must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 3.4.2 will apply to the re-submitted plan;
- 6.8 The rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

- 6.9 If the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

## **7.** Security Management Plan

### *Preparation of Security Management Plan*

- 7.1 This Paragraph 7 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
- 7.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule Appendix 1 (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.
- 7.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

an assessment of the Supplier Information Management System against the requirements of this Schedule Appendix 1 (Security Management), including the Annexes;

the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and

the following information in respect of each Sub-contractor:

#### **the Sub-contractor's:**

1. **Legal name;**
2. **Trading name (if any);**
3. **Registration details (where the Sub-contractor is not an individual);**

**the Sites used by the Sub-contractor;**

**the Buyer Data Processed by the Sub-contractor;**

**the Processing that the Sub-contractor will undertake in respect of the Buyer Data;**

**the measures the Sub-contractor has in place to comply with the requirements of this Schedule Appendix 1 (Security Management).**

- 7.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

- 7.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

*Updating Security Management Plan*

- 7.6 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

*Monitoring*

- 7.6 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
- a significant change to the components or architecture of the Supplier Information Management System;
  - a new risk to the components or architecture of the Supplier Information Management System;
  - a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;
  - a change in the threat profile;
  - a significant change to any risk component;
  - a significant change in the quantity of Personal Data held within the Service;
  - a proposal to change any of the Sites from which any part of the Services are provided; and/or
  - an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
- 7.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

## ANNEX 1: SECURITY REQUIREMENTS

### 1. Location

- 1.1 Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer Data either:

In the United Kingdom;

The European Economic Area; or

In a facility operated by an entity where:

1. **The entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable) containing the Standard Contractual Clauses;**
2. **The Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the Standard Contractual Clauses;**
3. **The Supplier has provided the Buyer with such information as the Buyer requires concerning:**
  1. **The entity;**
  2. **The arrangements with the entity; and**
  3. **The entity's compliance with the Standard Contractual Clauses; and**
4. **The Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.**

- 1.2 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.1:

it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and

the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.

- 1.3 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer Data as specified in the notice (a "**Prohibited Activity**").

1.3.1 in any particular country or group of countries;

1.3.2 in or using facilities operated by any particular entity or group of entities; or

- 1.3.3 in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a **"Prohibition Notice"**).
- 1.4 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

## 2 Vetting, Training and Staff Access

### *Vetting before performing or managing Services*

- 2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:

That individual has passed the security checks listed in paragraph 2.2; or

The Buyer has given prior written permission for a named individual to perform a specific role.

- 2.2 For the purposes of paragraph 2.1, the security checks are:

The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

2.2.1 **The individual's identity;**

2.2.2 **The individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;**

2.2.3 **The individual's previous employment history; and**

2.2.4 **That the individual has no Relevant Convictions;**

National security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

Such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

### *Annual training*

3. The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
1. General training concerning security and data handling; and
  2. Phishing, including the dangers from ransomware and other malware;



*Staff access*

**4.** The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

**5.** The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

**6.** Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

*Exception for certain Sub-contractors*

**7.** Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

As soon as practicable, and in any event within 5 Working Days of becoming aware of the issue, notify the Buyer;

Provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and

Comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

**8 Security Testing**

**8.1** This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

**Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.

**8.2** The Supplier must, at the Buyer's option, before providing the Services and when reasonably requested by the Buyer, either:

Conduct security testing of the Supplier Information Management System by:

**engaging a CHECK Service Provider or a CREST Service Provider;**

**designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and**

**providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within 10 Working Days of its receipt by the Supplier; or**

Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer's request or the Effective Date (as appropriate), including:

**the parts of the Supplier Information Management System tested;**

**a full, unedited and unredacted copy of the testing report; and**

**the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and**

**the Supplier's progress in implementing that remediation plan.**

8.3 The Supplier must remediate any vulnerabilities classified as "medium" or above in the security testing:

before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;

where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:

**by the date agreed with the Buyer; or**

**here no such agreement is reached:**

1. **within 5 Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;**
2. **within 1 month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and**
3. **within 3 months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.**

## 9 End-user Devices

9.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:

the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

users must authenticate before gaining access;

all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;

the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;

the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;

all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

9.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

9.3 Where there any conflict between the requirements of this Schedule Appendix 1 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

## 10. Encryption

10.1 Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:

When stored at any time when no operation is being performed on it; and

When transmitted.

10.2 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:

immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

10.3 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

10.4 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

10.5 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

The subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;

The protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

- 10.6 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to Cabinet Office Digital.

## 11. Access Control

- 11.1 The Supplier must, and must ensure that all Sub-contractors:
- identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
  - require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
  - allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
  - maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
- 11.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
- are accessible only from dedicated End-user Devices;
  - are configured so that those accounts can only be used for system administration tasks;
  - require passwords with high complexity that are changed regularly;
  - automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
- 11.3 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
- 11.4 The Supplier must, and must ensure that all Sub-contractors:
- configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
  - change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

## 12. Malicious Software

- 12.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
- 12.2 The Supplier shall ensure that such Anti-virus Software:

is configured to perform automatic software and definition updates;

performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

12.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

12.4 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 7.3 shall be borne by the parties as follows:

by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

by the Buyer, in any other circumstance.

### 13. Breach of Security

13.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

13.2 The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:

minimise the extent of actual or potential harm caused by such Breach of Security;

remedy such Breach of Security to the extent possible;

apply a tested mitigation against any such Breach of Security; and

prevent a further Breach of Security in the future which exploits the same root cause failure;

13.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

13.4 The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.

### 14. Sub-contractors

14.1 The Supplier must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the

people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer's request.

#### 14.2 **Third-party Software**

14.2.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.

#### 15. Deletion of Buyer Data

15.1 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

## Call Off Appendix 2

# Cabinet Office Environmental Policy Statement

The Cabinet Office recognises its potential to impact the environment, positively or negatively, directly or indirectly, through its activities and services.

The department is committed to continually improving its environmental performance for the scope of its ISO14001:2015 certification, by, where possible, preventing pollution and protecting the environment from negative impacts, while ensuring compliance, as a minimum, with all legal and other obligations.

To support this commitment, the department operates an Environmental Management System (EMS) covering its London estate and conducts regular and independent audits against the requirements of the ISO 14001:2015 standard.

The EMS covers activities related to the provision of office functions for policy staff and ministerial functions; including building and grounds maintenance; provision of supplies for offices; Chief Digital & Information Officer (CDIO) services; soft facilities management services.

EMS Objectives will as a minimum deliver on the targets set out in the Greening Government Commitments. This includes:

- protecting the environment
- reducing carbon emissions associated with our buildings and business travel
- reducing waste and increasing reuse and recycling opportunities
- using water more efficiently
- making use of technology to reduce environmental impact
- engaging with stakeholders to improve environmental performance, including in our supply chain

We will continually monitor performance against these objectives and the requirements of the ISO14001:2015 standard.

