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

Order Form

CALL-OFF REFERENCE:	VOA/2022/046
THE BUYER:	Valuation Office Agency (VOA)
BUYER ADDRESS	10 South Colonnade, London, E14 4PU
THE SUPPLIER:	Moorhouse Consulting Ltd
SUPPLIER ADDRESS:	
	Dashwood House, 16th Floor, 69 Old Broad St, London EC2M 1QS
REGISTRATION NUMBER:	05053551
DUNS NUMBER:	737971072
SID4GOV ID:	**N/A**

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated 17/02/2023.

It's issued under the Framework Contract with the reference number RM6187 for the provision of Professional Services to support the development of a new Future State design for the Agency

CALL-OFF LOT(S): Lot 2

Call-off incorporated terms

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

Where schedules are missing below, 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 7 (Financial Difficulties)- Optional
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 3 (Continuous Improvement)
- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 6 (ICT Services)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 20 (Call-Off Specification)
- Call-Off Schedule 23 (HMRC Terms)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility)
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

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1 - The Buyer is only liable to reimburse the Supplier for any expense

or any disbursement which is

(i) specified in this Contract or
(ii) which the Buyer has Approved prior to the Supplier incurring that expense or that disbursement. The Supplier may not invoice the Buyer for any other expenses or any other disbursements

Call-off start date: **27/02/2023**

Call-off expiry date: **15/05/2023**

Call-off initial period: **11 Weeks**

The buyer retains the right to extend by a minimum period of 4 weeks, and a further final extension of 4 weeks.

Call-off deliverables:
See details in Call-Off Schedule 20 (Call-Off Specification)

Security
Short form security requirements apply as per Call-Off Schedule 9.

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: £198,270

Call-off charges

See details in Order Schedule 5 (Pricing Details), which include the pricing proposal submitted by The Supplier as part of the tender bid.

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

Payments will be made on a per service basis, following commencement of the contract and dependent on satisfactory performance management.
Payments will be made via an electronic payments system, SAP Ariba P2P (MYBuy). Invoices should be provided for each milestone within one month of agreement of deliverables and sent to **REDACTED** copying in contract manager email address (and including the purchase order provided). Payments will be made into the bank account provided by the supplier.

Buyer's invoice address
REDACTED

FINANCIAL TRANSPARENCY OBJECTIVES
The Financial Transparency Objectives do apply to this Call-Off Contract.

Buyer's authorised representative

REDACTED

Buyer's security policy
None in addition to framework requirements

Supplier's authorised representative

REDACTED

Supplier's contract manager

REDACTED

Progress report frequency
Supplier to share progress reports by email to Buyer's Authorised Representative on a weekly basis. Short follow-up calls may be required to discuss points raised in the email.

Progress meeting frequency

Initial contract management meeting to take place within 2 weeks from the Order Start Date, where the Frequency of follow up meetings required will be agreed by both parties. This is separate to the kick-off meeting to take place in week one (1) of Order Start Date.

Key staff

REDACTED

Key subcontractor(s)
N/A

Commercially sensitive information

Information Class: Commercial Interests – rate card
Exemption (section of the Act): 43 Section 2
Detailed Reason for Application: Our commercial offer holds commercially sensitive information
Duration: 2 years

Service credits
N/A

Additional insurances
N/A

Guarantee
N/A

Buyer's environmental and social value policy
Appended at Appendix A

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:

REDACTED

For and on behalf of the Buyer:

REDACTED

Appendix A

Environmental Policy
It is the policy of the Valuation Office Agency to maintain an environmental system designed to meet the requirements of ISO14001:2015 (or any other standard in line with Annex SL Structure) in pursuit of its primary objectives, the purpose and the context of the organisation.

The VOA understands the importance of reducing the carbon footprint principally through the use of its estate, using its expertise to demonstrate its commitment to mitigating risk from climate change impacts, through compliance with legislation and regulations, adaptation, and adopting best practice.
The VOA Estates Team adopt an innovative approach to both technology and communication as well as more traditional methods, to encourage awareness of the sustainability policy Agency wide.
Additionally we align our aims and activities alongside our sponsor department HMRC, collaborating with them in our promise to adopt the following
These are as follows:

1. Regularly review how we use our estates, identify where efficiencies can be made and work towards improving our sustainability performance
2. We will continue to meet all current and foreseen legal requirements and related official codes of practice, and require our suppliers to do the same.
3. Achieve reduction in greenhouse gas emissions
4. Achieve savings in water consumption
5. Improve our diversion of waste from landfill to recycling
6. Where we share space, look to partner other government departments in developing and implementing estate sustainability initiatives
7. Encourage our people to use public transport when commuting to their place of work and between work locations.
8. Ensure that the goods and services we purchase support our environmental objectives wherever practicable and that we encourage our suppliers and contractors to improve their own environmental performance
9. Look for opportunities to sustain and enhance biodiversity across the estate
10. Effectively communicate with all colleagues and contractors on environmental policy and performance
11. Identify and provide appropriate training, advice and information for colleagues, encouraging an appetite for continuous improvement in our sustainability
12. Publish online our progress towards environmental sustainability

The VOA Estates Sustainability Manager is the VOA's professional expert with responsibility for advising and informing on environmental matters. All colleagues and contractors are expected to follow the principles of this policy and related guidance, and to assist in meeting the VOA's environmental sustainability objectives. This policy will be reviewed and assured at regular intervals.

Customer and stakeholder satisfaction is an essential part of the environmental process, to ensure this is fulfilled the Estates team receive training to ensure awareness and understanding of the environment and its impact of the products or service in which we provide.

To certify the Agency maintains its awareness for continuous improvement, the environmental system is regularly reviewed by Senior Leadership to ensure it remains appropriate and suitable to our business. The Environmental System is

subject to both internal and external annual audits.

Call-Off Schedule 4 (Call Off Tender)

The Supplier's bid proposal dated 30/01/23 and the Supplier's clarification dated 22/02/2023 and 23/02/2023 has been included below:

Supplier's bid:

REDACTED

Bid Clarification & Supplier's Response

Question	Answer
REDACTED	REDACTED
REDACTED	REDACTED.

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):

"Processor Personnel"	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.

The contact details of the Relevant Authority's Data Protection Officer are:

REDACTED

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

REDACTED

2.

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**REDACTED**
Duration of the Processing	**REDACTED**
Nature and purposes of the Processing	**REDACTED**
Type of Personal Data	**REDACTED**

Categories of Data Subject	**REDACTED**
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	**REDACTED** .

Annex 2 - Joint Controller Agreement – <u>not used</u>

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. 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.

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. 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.

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. 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.

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. 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. 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).
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.
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.

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. 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 5 (Pricing Details)

REDACTED

Call-Off Schedule 9 (Security)

Part A (Short Form Security Requirements) should apply.

Part A: Short Form Security Requirements

1. **Definitions**

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

"Breach of Security"	1. the occurrence of: 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 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, 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;
"Security Management Plan"	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.

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

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. 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.

3. Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

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.
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**

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.
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:
    1. is in accordance with the Law and this Contract;
    2. as a minimum demonstrates Good Industry Practice;
    3. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
    4. where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
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.
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**

1. **Introduction**
    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.
2. **Content of the Security Management Plan**
    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.

3. **Development of the Security Management Plan**

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.

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.

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. 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. **Amendment of the Security Management Plan**

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.
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.
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. 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**

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.

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:

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.

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.

Part B: Long Form Security Requirements – not used

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

REDACTED