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

Order Form

CALL-OFF REFERENCE:	**P1545** **REDACTED TEXT FOIA Section 31, Law Enforcement**
THE BUYER:	**His Majesty's Treasury**
BUYER ADDRESS	**1 Horse Guards Rd, London, SW1A 2HQ**
THE SUPPLIER:	**Oliver Wyman**
SUPPLIER ADDRESS:	**1 Tower Place West, Tower Place** **London** **EC3R 5BU**
REGISTRATION NUMBER:	03023304
DUNS NUMBER:	775403439

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated 19/02/2024.
It's issued under the Framework Contract with the reference number RM6187 for the provision of Management Consultancy Services to support OFSI Research and Industry Engagement.

CALL-OFF LOT(S):
Lot 3: Complex & 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:

This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.

1. Joint Schedule 1(Definitions and Interpretation) RM6187

2. 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)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 20 (Call-Off Specification)

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

1. The parties have agreed that for **15.2 of Call-Off Schedule 20 (Call-Off Specification)**, only Cyber Essential is required instead Cyber Essential Plus providing the Supplier holds both Cyber Essentials and ISO27001 certification in its performance of the services under this agreement.

2. The Buyer has agreed that **15.3 of Call-Off Schedule 20 (Call-Off Specification)** does not apply. The result of the penetration test dated 26th February 2024 provided was deemed to have satisfied this requirement.

3. The Buyer has agreed that the supplier can use EU-based data centres with ISO27001 accreditation for the purpose of **15.6 of Call-Off Schedule 20 (Call-Off Specification)** and the performance of the services under this agreement. The Supplier has agreed that only open source data will be kept or processed on the Supplier's laptops. All Buyer's data, or sensitive data will be processed by Supplier staff with SC clearance on laptops provided by the Buyer.

Call-off start date: 19/02/2024

Call-off expiry date: 18/08/2024

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

CALL-OFF OPTIONAL EXTENSION PERIOD

The Buyer has the right to extend the contract by 2 separate 1 month period (1 month + 1 month)

Call-off deliverables:

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

Security

Long form security requirements apply.

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:

Estimated Year 1 Charges of the Contract including extension options are £622,920 (excluding VAT)

Call-off charges

The overall call-off charges shall be capped at £622,920 (excluding VAT)

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

Reimbursable expenses

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

Payment method

Payment will be made by BACS and can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

Buyer's invoice address

Accounts Payable
HM Treasury
Rosebery Court, St Andrew's Business Park, Norwich, NR7 0HS
Invoicequeries@hmtreasury.gov.uk

FINANCIAL TRANSPARENCY OBJECTIVES
Not applicable

Buyer's authorised representative

REDACTED TEXT FOIA Section 40, Personal Information

Supplier's authorised representative

REDACTED TEXT FOIA Section 40, Personal Information

Supplier's contract manager

REDACTED TEXT FOIA Section 40, Personal Information

Progress report frequency
Not applicable

Progress meeting frequency
Not applicable

Key staff

REDACTED TEXT FOIA Section 40, Personal Information

Key subcontractor(s)
Not applicable

Commercially sensitive information
Not applicable

Service credits
See details in Call-Off Schedule 20 (Call-Off Specification) section 14.

Additional insurances
Not applicable

Guarantee
Not applicable

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.

Signed - via Docusign
Supplier **REDACTED TEXT FOIA Section 40, Personal Information**
REDACTED TEXT FOIA Section 40, Personal Information

Buyer
REDACTED TEXT FOIA Section 40, Personal Information
REDACTED TEXT FOIA Section 40, Personal Information

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.

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are: **REDACTED TEXT FOIA Section 40, Personal Information**

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **REDACTED TEXT FOIA Section 40, Personal Information**, Email: **REDACTED TEXT FOIA Section 40, Personal Information.**

1.1.1.3 The Supplier shall comply with any further written instructions with respect to Processing by the Controller.

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Personnel, for which the Supplier is the Controller ● Business contact details of the Relevant Authority engaged in the performance of the Relevant Authority's duties under the Contract, for which the Relevant Authority is the Controller ● Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority
Duration of the Processing	Personal data processed for the purposes of fulfilment of the Services will only be held by the Supplier and the Relevant Authority for the duration of the contract and during any Services provided after termination. Personal Data appearing in open-source information provided by the Supplier to the Relevant Authority, as part of the Service, will be

	processed by the Relevant Authority for as long as it is required for its business purposes in accordance with the Data Protection Legislation.
Nature and purposes of the Processing	Business contact details of the Supplier and the Relevant Authority will be processed for the purposes of the Services provided by the Supplier for business engagement purposes (i.e., enabling individuals from each Party to successfully engage with relevant individuals in the other). Any Personal Data appearing in open-source information shared by the Supplier with the Relevant Authority will be processed by the Relevant Authority in order for it to pursue its aims and objectives in relation to the implementation and enforcement of financial sanctions in the United Kingdom. Where necessary, as a result of information provided by the Supplier, this may lead to the sharing of the open-source Personal Data received with relevant government departments and law enforcement agencies in furtherance of their regulatory activities.
Type of Personal Data	Business contact details of the Supplier and the Relevant Authority are likely to include, but not be limited to, name, role, business email address, business telephone number etc. Any Personal Data appearing in open-source information shared by the Supplier with the Relevant Authority is likely to include, but not be limited to, name and the reason(s) for the data subjects' relevance to the open-source information being shared with the Relevant Authority.
Categories of Data Subject	• Relevant employees of the Supplier involved in the supply of the Services • Relevant employees of the Relevant Authority receiving information for the purpose of the Services • Any living individuals identifiable from open-source information shared by the Supplier with the Relevant Authority in fulfilment of the Services
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under	Personal data processed for the purposes of the Services will only be held by the Supplier and the Relevant Authority for the duration of the contract and during any Services provided after termination. Once no longer required for the purpose of the Services, these personal data will be securely destroyed by both Parties. Any Personal Data appearing in open-source information shared by the Supplier with the Relevant Authority will be stored by the

Union or Member State law to preserve that type of data	Relevant Authority for as long as required to meet its business purposes, after which time it will be securely destroyed.

Call-Off Schedule 5 (Pricing Details)

Procurement name:	**Management Consultancy ~~for OFSI~~**

Procurement reference:	**ITT_46369**

RM6187 Lot number	**Lot 3**

Supplier to insert name	**Oliver Wyman**

If your project is split into numerous activities which you would like priced separately please include below	Price
	Total fixed price
Total fixed price including all expenses but excluding VAT	**£622,920.00**

Procurement name:	**REDACTED TEXT FOIA Section 31, Law Enforcement**

Procurement reference:	**ITT_46369**
RM6187 Lot number	**Lot 3**

Supplier to insert name	**Oliver Wyman**

TOTAL				**£622,920**	
Grade	**Names**	**Daily Rate (£ exc VAT)**	**Number of days**	**Total**	**Weighting (%)**
Partner	**REDACTED TEXT FOIA Section 40, Personal Information**	**REDACTED TEXT FOIA Section 43, Commercial interests**	**REDACTED TEXT FOIA Section 43, Commercial interests**	**REDACTED TEXT FOIA Section 43, Commercial interests**	
Partner	**REDACTED TEXT FOIA Section 40, Personal Information**	**REDACTED TEXT FOIA Section 43, Commercial interests**	**REDACTED TEXT FOIA Section 43, Commercial interests**	**REDACTED TEXT FOIA Section 43, Commercial interests**	
Partner	**REDACTED TEXT FOIA Section 40, Personal Information**	**REDACTED TEXT FOIA Section 43,**	**REDACTED TEXT FOIA Section 43,**	**REDACTED TEXT FOIA Section 43,**	

		Commercial interests	Commercial interests	Commercial interests	
Partner	REDACTED TEXT FOIA Section 40, Personal Information	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	
Principal Consultant / Associate Director	REDACTED TEXT FOIA Section 40, Personal Information	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	
Senior Consultant / Engagement Manager / Project Lead	REDACTED TEXT FOIA Section 40, Personal Information	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	
Consultant	REDACTED TEXT FOIA Section 40, Personal Information	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	REDACTED TEXT FOIA Section 43, Commercial interests	

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)

1. Definitions

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

1. "Breach of Security"	1 means the occurrence of: a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
2. "ISMS"	3 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
3. "Security Tests"	4 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

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

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

2.3 The Parties shall each appoint a security representative to be responsible for Security.

The initial security representatives of the Parties are:

2.3.1 **REDACTED TEXT FOIA Section 40, Personal Information**

2.3.2 **REDACTED TEXT FOIA Section 40, Personal Information**

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

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

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

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

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

3. Information Security Management System (ISMS)

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

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

3.3 The Buyer acknowledges that;

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

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

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's

Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

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

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

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

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

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

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

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

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

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

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly

have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

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

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

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

any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

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

5. Amendment of the ISMS and Security Management Plan

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

- 5.1.1 emerging changes in Good Industry Practice;
- 5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
- 5.1.3 any new perceived or changed security threats;
- 5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
- 5.1.5 any new perceived or changed security threats; and
- 5.1.6 any reasonable change in requirement requested by the Buyer.

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

- 5.2.1 suggested improvements to the effectiveness of the ISMS;
- 5.2.2 updates to the risk assessments;
- 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
- 5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually

across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

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

7. Complying with the ISMS

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

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

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

8. Security Breach

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

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

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

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably

related to a possible incident or compromise); and

f) as soon as reasonably practicable, provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

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

9. Vulnerabilities and fixing them

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

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

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

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

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

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

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

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

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the

release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

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

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

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

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

4.

1. Handling Classified information

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

2. End user devices

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

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

3. Data Processing, Storage, Management and Destruction

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

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

3.3 The Supplier shall:

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

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated

privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

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

8. Audit

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

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

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

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

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

Part B – Annex 2 - Security Management Plan

[ ]

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

"Exclusive Assets"	1 Supplier Assets used exclusively by the Supplier a Key Subcontractor in the provision of the Deliverables;
"Exit Information"	2 has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	3 the person appointed by each Party to manage their respective obligations under this Schedule;
“Exit Plan”	4 the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	5 the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	6 those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes;
"Registers"	7 the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	8 any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	9 any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date,

	whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	10 the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	11 has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	12 the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	13 Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	14 Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	15 has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	16 has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for contract exit

2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty

(20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every six (6) months throughout the Contract Period; and

(b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than twenty (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier,

provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Subcontract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

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

1. Definitions

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

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

Project Management

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.

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.

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

Role of the Supplier Contract Manager

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

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;

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;

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

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

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.

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.

Role of the Operational Board

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.

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.

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.

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.

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.

Contract Risk Management

Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

the identification and management of risks;

the identification and management of issues; and

monitoring and controlling project plans.

The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer and the Supplier have identified.

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

Contract Reference: P1545

Office of Financial Sanctions Implementation Threat Assessment +

CONTENTS

1. PURPOSE

1.1. HM Treasury **REDACTED TEXT FOIA Section 31, Law Enforcement** 'the Buyer' requires external management consultancy support to manage and deliver several workstreams **REDACTED TEXT FOIA Section 31, Law Enforcement.**

2. BACKGROUND TO THE BUYER

2.1. HM Treasury is the government's economic and finance ministry, maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth. **REDACTED TEXT FOIA Section 31, Law Enforcement**

2.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
3.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
3.3. **REDACTED TEXT FOIA Section 31, Law Enforcement**

4. DEFINITIONS

Expression or Acronym	Definition
REDACTED TEXT FOIA Section 31, Law Enforcement	**REDACTED TEXT FOIA Section 31, Law Enforcement**
SC	Security Check
GDPR	General Data Protection Regulation

5. SCOPE OF REQUIREMENT

5.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
5.1.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
5.1.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
5.1.3. **REDACTED TEXT FOIA Section 31, Law Enforcement**
5.1.4. **REDACTED TEXT FOIA Section 31, Law Enforcement**

6. THE REQUIREMENT

6.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.1.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.1.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.1.3. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.1.4. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.1.5. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.2.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.3. **REDACTED TEXT FOIA Section 31, Law Enforcement**

6.3.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.3.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.4. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.4.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.5. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.5.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.5.2. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.5.3. **REDACTED TEXT FOIA Section 31, Law Enforcement**
6.6. Security:
6.6.1. See section 15 for security requirements.
6.7. Other:
6.7.1. **REDACTED TEXT FOIA Section 31, Law Enforcement**

7. KEY MILESTONES AND DELIVERABLES

7.1. The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	**REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement**
2	**REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement**
3	**REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement**
4	**REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement**
5	**REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement**

REDACTED TEXT FOIA Section 31, Law Enforcement

8. MANAGEMENT INFORMATION/REPORTING

8.1. Fortnightly reports of progress and quality assurance of outputs.

9. CONTINUOUS IMPROVEMENT

9.1. The Supplier will be expected to continually improve the way in which the required services are to be delivered throughout the contract duration.
9.2. The Supplier should identify and present any new and beneficial ways of working to **REDACTED TEXT FOIA Section 31, Law Enforcement** staff during review meetings.
9.3. Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

10. SOCIAL VALUE & SUSTAINABILITY

10.1. Procurement of a solution meeting the requirement as outlined above would align with the Public Services (Social Value) Act 2012 by increasing supply chain capacity.

10.2. The solution shall tackle economic inequality by increasing supply chain resilience and capacity. In particular, the solution will: support innovation and disruptive technologies throughout the supply chain to deliver lower cost and/or higher quality goods and services; and support the development of scalable and future-proofed new methods to modernise delivery and increase productivity.

10.3. The supplier should refer to Procurement Policy Note (PPN) 06/20 for further guidance:

https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts

10.4. The supplier shall meet the applicable Government Buying Standards applicable to deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

11. QUALITY

11.1. The specialist support provided by the successful supplier should be of a high standard with key quality outputs forming part of the delivery of the requirement. Specific quality expectations will be agreed as part of supplier mobilisation post contract award.

12. PRICE

12.1. Potential Suppliers are requested to provide a rate card (both for hourly and daily rates) for work that may arise during the contract. Where possible, the rate card for this requirement should include a discount on the Supplier's standard rate card for this Lot. This rate card may be used by the Authority to pay on a resource consumption basis, or to fix a capped fee for larger pieces of work or in respect of particular instructions.

12.2. All further ad hoc work is subject to requirements arising, and any costs incurred must be agreed with the Authority in writing prior to being incurred, or the Authority is not obligated to meet these costs.

12.3. Bids will be evaluated on a most economically advantageous tender basis.

12.4. Prices are to be submitted via the e-Sourcing Suite [Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery

13. STAFF AND CUSTOMER SERVICE

13.1. The Supplier shall provide a sufficient level of capable resource throughout the duration of the contract to consistently deliver a high-quality service.

13.2. The Supplier's staff assigned to the contract shall have the relevant qualifications and experience to deliver the contract to the required standard.

13.3. The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the contract.

14. SERVICE LEVELS AND PERFORMANCE

14.1. The Supplier shall provide a sufficient level of capable resource throughout the duration of the Contract to consistently deliver a high-quality service.

14.2. The Supplier's staff assigned to the contract shall have the relevant qualifications and experience to deliver the contracted service to the required standard.

14.3. The supplier must provide an escalation point to resolve any issues with the availability of the service.

14.4. In the event of termination of the contract the Supplier must provide a complete copy of all data and documents held within the system in a format and timescale that is acceptable to the Buyer and which will be agreed during contract mobilisation. Once this transfer has been validated by the Buyer, the Supplier must ensure that its copies of all the data and documents are deleted.

14.5. The Buyer will measure the quality of the Supplier's delivery by:

KPI/ SLA	Service Area	KPI/SLA description	Performance Target	Service Credits (each service period)
1	Innovation	The Supplier should demonstrate the ability to deliver against the requirement at each stage of deliver. The Supplier will suggest new ways of working and work collaboratively **REDACTED TEXT FOIA Section 31, Law Enforcement** to refine the full requirement as needed.	**REDACTED TEXT FOIA Section 31, Law Enforcement** survey undertaken. 80% of responses should be 'satisfactory' or above (poor, unsatisfactory, satisfactory and excellent).	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
3	Engagement	The Supplier will work collaboratively **REDACTED TEXT FOIA Section 31, Law Enforcement**	**REDACTED TEXT FOIA Section 31, Law Enforcement** survey undertaken. 80% of responses should be 'satisfactory' or above (poor, unsatisfactory, satisfactory and excellent).	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure.
4	Commercial	The Supplier will deliver required products within a budget agreed in advance **REDACTED TEXT FOIA Section 31, Law Enforcement**	100%	
5	Delivery	The Supplier will deliver the required products within the suggested timeframe.	100%	

Social value KPI/s is to be agreed with supplier on contract mobilization.

15. SECURITY AND CONFIDENTIALITY REQUIREMENTS

15.1. Suppliers must be able to demonstrate compliance with the Government Security Policy Framework and that they have appropriate IT, physical, personnel and procedural security measures in place to prevent any unauthorised access to, or leakage of, data collected as part of this contract, and to prevent it being shared with any unauthorised third parties. Such security measures should comply with the requirements of the ISO27001 standard as a minimum and the Buyer would wish to see evidence of that compliance, e.g., in the form of current ISO 27001 certification.

15.2. Any IT systems used by Suppliers to meet the Buyer's requirement must comply with National Cyber Security Centre (NCSC)'s 10 Steps to Cyber Security and with the NCSC's Cloud Security Principles. The Supplier should also hold NCSC's Cyber Essentials Plus certification and provide the Buyer with evidence of this.

15.3. Any IT systems that would be deployed by Suppliers to meet any part of the requirement must be subjected to periodic (at least annual) independent penetration testing and any significant vulnerabilities identified as part of the penetration testing must be remediated with timeframes agreed with the Buyer.

15.4. The Supplier should describe how, in order to ensure that reliance isn't placed solely on annual penetration testing to identify and address vulnerabilities, they might perform regular vulnerability scans on the component devices of the IT infrastructure and how they would ensure that any significant vulnerabilities identified by those scans are remediated as soon as possible.

15.5. Where any IT systems used by Suppliers to meet any part of the requirement need to generate any emails, the Supplier must be able to ensure that encryption and anti-spoofing measures can be applied to the emails which comply with the following guidance:

15.5.1. https://www.gov.uk/guidance/securing-government-email

15.6. Suppliers are expected to demonstrate they have appropriate physical security measures in place in any premises used to store/process the Buyer's data. As above such physical security measures should comply with the requirements of ISO27001 as a minimum. Any data centres used by the Supplier to meet the Buyer's requirement must hold current ISO27001 certification and be UK based.

15.7. Suppliers shall ensure that any suspected or actual security breaches related to Buyer's data/information are reported to the Buyer immediately. Where any actual security breaches have been identified, Suppliers shall, as soon as reasonably practicable, provide to the Buyer a report setting out the details of the security breach, including an impact assessment, a root cause analysis and of the steps taken to address the breach.

15.8. Full compliance with the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) is essential.

16. PAYMENT AND INVOICING

16.1. Payment can only be made following satisfactory delivery of pre-agreed deliverables.

16.2. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

16.3. Invoices should be submitted to: InvoiceQueries@hmtreasury.gov.uk.

17. CONTRACT MANAGEMENT

17.1. Attendance at Contract Review meetings shall be at the Supplier's own expense.

18. LOCATION

18.1. **REDACTED TEXT FOIA Section 31, Law Enforcement** 1 Horse Guards Road, London, SW1A 2HQ and Feethams, Darlington, DL1 5AD. The Supplier should be aware that staff are based at these offices but also work remotely in accordance with HMT guidelines.

Call-Off Schedule 4 (Call Off Tender)

HMT - MANAGEMENT CONSULTANCY SERVICES **REDACTED TEXT FOIA Section 31, Law Enforcement**

Oliver Wyman – Qualification Envelope

12 January 2024

QUALIFICATION - KEY PARTICIPATION REQUIREMENTS

Response Guidance

The following questions are 'Pass/Fail' questions. If Potential Bidders are unwilling or unable to answer "Yes", their submission will be deemed non-compliant and shall be rejected.

Potential Bidders should confirm their answer by selecting the appropriate option.

Please submit your response to all questions in the Qualification Envelope in a single attachment.

Question Number	Question	Your Response
1.1	Do you accept the competition rules as described in Attachment 1 – About the Procurement?	**Yes**
1.2	Have you read, understood and accepted the Bid Pack and all associated attachments, specifically Attachment 3 - Statement of Requirements?	**Yes**
1.3	Do you agree, without caveats or limitations, that in the event that you are successful, **RM6187 Management Consultancy Framework 3** Call-off Terms will govern the provision of this contract?	**Yes**
1.4	Do you confirm your Organisation's e-Sourcing suite profile is complete and accurate at the time the bid closed and that any amendments made following acceptance of this event will be notified to the buyer in writing?	**Yes**

Qualification - Conflicts of Interest
Response Guidance

Question 2.1 is a 'Yes/No' question and will dictate whether or not question 2.2 needs to be answered.

Question 2.2 is a Pass / Fail question that only needs to be answered where you have answered 'Yes' in question 2.1.

Potential Bidders are required to provide details of how the identified conflict will be

mitigated.

The Contracting Authority will review the mitigation in line with the perceived conflict of interest, to determine what level of risk this poses to them. Therefore, if Potential Bidders cannot or are unwilling to suitably demonstrate that they have suitable safeguards to mitigate any risk then their Bid will be deemed non-compliant and will be rejected.

Please submit your response to all questions in the Qualification Envelope in a single attachment.

Question Number	Question	Your Response
2.1	Please confirm whether you have any potential, actual or perceived conflicts of interest that may be relevant to this requirement.	**No**
2.2	We require that any potential, actual or perceived conflicts of interest in respect of this Bid Pack are identified in writing and that companies outline what safeguards would be put in place to mitigate the risk of actual or perceived conflicts arising during the delivery of these services.	**N/A**

Qualification - Information only
Response Guidance
The following questions are for information only and do not form part of the evaluation. Information provided in response to these questions may be used in preparation of any Contract Award and any omissions may delay completion of this procurement.

Please submit your response to all questions in the Qualification Envelope in a single attachment.

Question Number	Question	Your Response
3.1	Please provide details of where the Award Outcome should be directed. Your response must include their; a. Full Name: Anthony Charrie b. Role/Title c. Registered Address d. Email Address	**REDACTED TEXT FOIA Section 40, Personal Information**
3.2	Please provide details of any subcontractors you propose to use in order to meet your obligations should you be awarded a Contract. Your response must include their; a. Organisation Name(s) b. Company Registration Number c. Registered Address(ees) d. Contact Details e. Services to be provided	N/A

HMT - MANAGEMENT CONSULTANCY SERVICES **REDACTED TEXT FOIA Section 31, Law Enforcement**

Oliver Wyman – Technical Response

31 January 2024

Appendix A. **CONFIDENTIALITY**

1) Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

2) Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies, and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.

3)

Appendix B. Contents

Q4.1. Comprehensive and high quality open-source research

REDACTED TEXT FOIA Section 43, Commercial interests

Q4.2. Outsourcing and overseeing delivery of rigorous, targeted research to external SMEs

REDACTED TEXT FOIA Section 43, Commercial interests

Q4.3. Deliver engagement with relevant private stakeholders

4) **REDACTED TEXT FOIA Section 43, Commercial interests**

Q4.5 Project management

5) **REDACTED TEXT FOIA Section 43, Commercial interests**

Q5 Past Experience

REDACTED TEXT FOIA Section 43, Commercial interests

Q6 Social Value - Tackling Economic Inequality

REDACTED TEXT FOIA Section 43, Commercial interests

Annex A

REDACTED TEXT FOIA Section 43, Commercial interests

AND

REDACTED TEXT FOIA Section 40, Personal Information