Crown Commercial Service

CONSTRUCTION PROFESSIONAL SERVICES FRAMEWORK SCHEDULE 5

TEMPLATE CALL OFF AGREEMENT (INCORPORATING THE NEC4 PROFESSIONAL SERVICES SHORT CONTRACT JUNE 2017 (INCLUDING AMENDMENTS ISSUED JANUARY 2019 AND OCTOBER 2020) AND CONTRACT DATA

Date: 18/07/2023

FORM OF AGREEMENT

Incorporating the NEC4 Professional Services Short Contract June 2017 incorporating amendments January 2019 and October 2020

Between

Valuation Office Agency

And

FAITHFUL + GOULD LIMITED

For the provision of

a Contract to supply

Building Surveyor advice to the Valuation Office Agency

Reference : VOA/2023/020

THIS AGREEMENT is made the 18th day of July 2023

PARTIES:

1. **Valuation Office Agency,** on behalf of the Commissioners of HMRC whose registered office is at 10 South Colonnade, London, E14 (the "***Client***"); and

2. **FAITHFUL + GOULD LIMITED** which is a company incorporated in and in accordance with the laws of England (Company No. 02236832) whose registered office address is at Woodcote Grove, Ashley Road, Epsom, Surrey, KT18 5BW (the "***Consultant***").

BACKGROUND

(A) The Minister for the Cabinet Office (the "**Cabinet Office**") as represented by Crown Commercial Service, a trading fund of the Cabinet Office, without separate legal personality (the "**Authority**"), established a framework for construction professional services for the benefit of public sector bodies.

(B) The *Consultant* was appointed to the framework and executed the framework agreement (with reference number RM6165) which is dated 01/10/2021 (the "**Framework Agreement**"). In the Framework Agreement, the Consultant is identified as the "Supplier".

(C) The *Consultant* has agreed to Provide the Services in accordance with this agreement and the Framework Agreement.

IT IS AGREED AS FOLLOWS:

1. The *Client* will pay the *Consultant* the amount due and carry out his duties in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.

2. The *Consultant* will Provide the Service in accordance with the *conditions of contract* identified in the Contract Data and the Contract Schedules.

   This contract incorporates the conditions of contract in the form of the NEC4 Professional Services Short Contract June 2017 Edition incorporating amendments January 2019 and October 2020 and incorporating the additional conditions specified in the Client's Contract Data, which form this contract together with the documents referred to in it. References in the NEC4 Professional Services Short Contract June 2017 Edition incorporating amendments January 2019 and October 2020 to "the contract" are references to this contract.

3. This contract [and the Framework Agreement] is the entire agreement between the parties in relation to the *service* and supersedes and extinguishes all prior arrangements, understandings, agreements, statements, representations or warranties (whether written or oral) relating thereto.

4. Neither party has been given, nor entered into this contract in reliance on any arrangements, understandings, agreements, statements, representations or warranties other than those expressly set out in this agreement.

5. Nothing in clauses 4 or 5 shall exclude liability in respect of misrepresentations made fraudulently.

Executed under hand

Signed by an authorized signatory/director for and on behalf of the *Client*; Valuation Office Agency, on behalf of the Commissioners of HMRC

Signature .....

Date .....

Name in Capitals .....

Signed by an authorized signatory/director for and on behalf of the *Consultant*; Faithful + Gould Limited

Signature .....

Date .....

Name in Capitals .....

Short Contract

A contract between

Valuation Office Agency

and

FAITHFUL + GOULD LIMITED

for

Pre-acquisition surveys of properties to be acquired for infrastructure schemes.

Contract Forms

Contract Data

The *Consultant's* Offer

Price List

Scope

Contract Data

The *Client's* Contract Data

The *Client* is

Name	**Valuation Office Agency**
Address for communications	8th Floor, 10 South Colonnade, Canary Wharf, London E14 4PU
Address for electronic communications	**REDACTED**
The service is	To undertake pre-acquisition surveys of properties to be acquired for infrastructure schemes. The condition surveys are visual only and 'non-intrusive' but look at the fabric, structure and services and highlighting any identified needs for repair and any potential issues, hazardous defects including any recommendations for further investigation. Full details and photographs are to be included in reports.
The starting date is	03/07/2023
The completion date is	02/07/2025
The delay damages are	N/A per day
The *law of the contract* is	England and Wales
The *period for reply* is	2 weeks
The *defects date* is	4 weeks after Completion
The *assessment date* is the	7th of each month

The United Kingdom Housing Grants, Construction and Regeneration Act (1996) **does** apply

The *Adjudicator* is:

Name	Not Named
Address for communications	N/A
Address for electronic communications	N/A

Contract Data

The *Client's* Contract Data

The interest rate on late payments is **REDACTED** % per complete week of delay

Insert a rate only if a rate less than 0.5% per week of delay has been agreed.

The *Client* provides this insurance

N/A

Only enter details here if the *Client* is to provide insurance.

The *Consultant* provides the following insurance cover

INSURANCE AGAINST	**MINIMUM AMOUNT OF COVER**	**PERIOD FOLLOWING COMPLETION OR EARLIER TERMINATION**
Liability of the *Consultant* for claims made against it arising out of the *Consultant's* failure to use the skill and care normally used by professionals providing services similar to the service.	£1,000,000* –minimum £1 million, in respect of any one occurrence claim arising out of the same original cause or source with lower annual and/or annual aggregate limits of cover in respect of claims relating to pollution contamination and similar where such limited cover is the norm without limit to the number of claims	**6 years**
Loss of or damage to property and liability for bodily injury to or death of a person (not an employee of the *Consultant)* arising from or in connection with the *Consultant* Providing the Service	£10,000,000* in respect of each claim occurrence, without limit to the number of claims occurrences	**6 years**
Liability for death of or bodily injury to employees of the *Consultant* arising out of and in the course of their employment in connection with the contract	The greater of the amount required by law and £10,000,000* in respect of each claim occurrence, without limit to the number of claims occurrences	**6 years**

The *Consultant's* total liability to the *Client* which arises under or in connection with the contract is limited to: £5,000,000

The *Adjudicator nominating body* is: the Royal Institution of Chartered Surveyors

The *tribunal* is: Courts of England and Wales

Contract Data

The *Client's* Contract Data

If the *tribunal* is arbitration, the arbitration procedure is	N/A

The *conditions of contract* are the NEC4 Professional Service Short Contract June 2017 incorporating amendments January 2019 and October 2020 and the following additional conditions

Only enter details here if additional conditions are required

Option Z2 Identified and defined terms

[applies]

Option Z4 Admittance to Client's Premises

[does not apply]

Option Z5 Prevention of fraud and bribery

[applies]

Option Z6 Equality and Diversity

[applies]

Option Z7 Legislation and Official Secrets

[applies]

Option Z8 Conflict of Interest

[applies]

Option Z9 Publicity and Branding

[applies]

Option Z10 Freedom of information

[applies]

Option Z14 Confidentiality and Information Sharing

[applies]

Option Z14 Security Requirements

[applies] – see Schedule 2

Option Z16 Tax Compliance

[applies]

Option Z22 Fair payment

[applies]

Option Z26 Building Information Modelling

[does not apply]

Option Z42 The Housing Grants, Construction and Regeneration Act 1996

[does not apply]

Option Z44 Intellectual Property Rights

[applies]

Option Z45 HMRC Requirements

[applies]

Option Z46 MoD DEFCON Requirements

[does not apply]

Option Z47 Small and Medium Sized Enterprises (SMEs)

[does not apply]

Option Z48 Apprenticeships

[applies]

Option Z49 Change of Control

[applies]

Option Z50 Financial Standing

[applies]

Option Z51 Financial Distress

[does not apply]

Option Z52 Records, audit access and open book data

[applies]

Option Z100 Data Protection

[applies] – See Schedule 1

Option Z101 Cyber Essentials

[does not apply]

Other additional conditions

[insert details/reference of any other additional conditions required by the Client]

Contract Data

The *Consultant's* Contract Data

The *Consultant* is

Name	Faithful + Gould
Address for communications	Two Chamberlain Square, Paradise Circus, Birmingham, B3 3AX
Address for electronic communications	**REDACTED**
The service is	Condition surveys
The starting date is	03/07/2023
The completion date is	02/07/2025
The delay damages are	N/A per day

The *fee percentage is* N/A %

The *people rates* are

category of person	unit	rate
See schedule of rates		

If the work is to be carried out on a time change basis the *Consultant* includes *people rates* for its own people as well as people provided by a subcontractor

The *key persons* are

Name	**REDACTED**
Job	**REDACTED**
Responsibilities	**REDACTED**
Qualifications	**REDACTED**
Experience	**REDACTED**

The *Consultant's* Offer

The *Consultant* offers to Provide the Service in accordance with these *conditions of contract* for an amount to be determined in accordance with these *conditions of contract*.

The offered total of the prices is	N/A

Enter the total of the Prices from the Price List. If all work is to be carried out on a time charge basis, enter 'Not Applicable'

Price List

1. **"The contract does not provide for the *Consultant* to be paid on a mixture of time charge and Prices and one or the other must be selected. If the work is to be paid on a time charge basis, only expenses should be included. No other entries should be made in the Price List. If the *Consultant* is to be paid on a priced basis the entries in the first four columns are made by the *Client* of the tenderer.**

2. **For each row:**

- **If the *Consultant* is to be paid an amount for the item which is not adjusted if the quantity of work in the item changes, the tenderer enters the amount in the Price column only.**
- **If the *Consultant* is to be paid an amount for the item of work and which is the rate for the work multiplied by the quantity completed, the tenderer enters the rate which is then multiplied by the expected quantity to produce the Price, which is also entered.**

3. **Costs incurred by the *Consultant* other than the listed expenses are included in the Rates and**
4. **Prices and the People Rates. If expenses are paid at cost, then 'at cost' should be entered into**
5. **the Rate column.**

Delete or strike through unused rows.

ITEM NUMBER	DESCRIPTION	UNIT	EXPECTED QUANTITY	RATE	PRICE
N/A					
			The total of the Prices		
EXPENSES					
Mileage	**REDACTED – Expenses will be paid as per VOA's Travel & Subsistence Policy**				

The method and rules used to compile the Price List are

REDACTED

Scope

6. **The Scope should be a complete and precise statement of the *Client's* requirements. If it is incomplete or imprecise, there is a risk that the *Consultant* will interpret it differently from the *Client's* intention. Information provided by the *Consultant* should be listed in the Scope only if the *Client* is satisfied that it is required, is part of a complete statement of the *Client's* requirements and is consistent with other parts of the Scope.**

1. Purpose of the *Service*

Provide a brief summary of why the *service* is being commissioned and what it will be used for.

The *Client* requires a fully qualified Chartered Building Surveying company to undertake primarily pre-acquisition surveys of properties to be acquired for infrastructure schemes. The condition surveys are visual only and 'non-intrusive' but look at the fabric, structure and services and highlighting any identified needs for repair and any potential issues, hazardous defects including any recommendations for further investigation. Full details and photographs are to be included in reports. Reports are required within 10 working days of instruction.

There may also be a requirement to undertake other building services ad-hoc work as per Framework services.

2. Description of the *service*

Give a complete and precise description of what the *Consultant* is required to do.

The *Client's* INVITATION TO TENDER SPECIFICATION dated 21/04/2023 has been included and Redacted

INVITATION TO TENDER

SPECIFICATION

For the provision of a Contract to supply

Building Surveyor advice to the Valuation

Office Agency

VOA Ref: VOA/2023/020

1. INTRODUCTION

1.1. The Valuation Office Agency (VOA) is an executive agency of HMRC with

circa 3,500 staff. Our main functions are to compile and maintain the business rating and council tax valuation lists for England and Wales, value property in England, Wales, and Scotland for the purposes of taxes administered by HMRC, provide statutory and non-statutory property valuation services in England, Wales, and Scotland, determine Local Housing Allowance levels, and register fair rents in England.

1.2. The Valuation Office Agency's rating and council tax valuations provide the base valuation data for the collection of around 51 billion of local taxation a year.

1.3. The work of the VOA encompasses:

• compiling and maintaining lists of rateable values of the 1.7 million nondomestic properties in England, and the 100,000 in Wales, to support the collection of around 25 billion1 in business rates;

• compiling and maintaining the lists of council tax bandings of some 23 million domestic properties in England and 1.3 million in Wales, to support the collection of around 26 billion2 in council tax;

• determining local housing allowances across some 150 Broad Rental Market areas for housing benefit purposes and registering some 60,000 Rent Act 1977 fair rents in England;

• delivering a range of statutory and non-statutory valuation and surveying services to central and local government departments and the wider public sector; and

• providing valuation advice to HMRC in connection with capital gains, inheritance tax and other tax compliance work.

1.4. Please see www.voa.gov.uk for further details

2. BACKGROUND

The VOA is a strategic supplier of land and property professional services to a number of infrastructure suppliers advising on, amongst other things, compulsory purchase, blight acquisitions and other compensation issues.

The VOA is a supplier for.

1. HS2 Phase 1 Framework. Mainly London fringe to Aylesbury Vale and rural Warwickshire but could be anywhere on Phase 1.
2. HS2 Phase 2 contract. Mainly North Derbyshire to Wakefield but could be anywhere on Phase 2.
3. National Highways - national contract.
4. Transport For Scotland.

REQUIREMENT

3.1. We require a fully qualified Chartered Building Surveying company to undertake primarily pre-acquisition surveys of properties to be acquired for infrastructure schemes. The condition surveys are visual only and 'nonintrusive' but look at the fabric, structure and services and highlighting any identified needs for repair and any potential issues, hazardous defects including any recommendations for further investigation. Full details and photographs are to be included in reports.

3.2. Reports are required within 10 working days of instruction.

3.3. There may also be a requirement to undertake other building services adhoc work as per Framework services.

4. CONFLICTS OF INTEREST

4.1. The Contractor shall not accept outside instructions to act against the VOA in circumstances where the matter relates to the subject matter of the contract awarded.

4.2. The Contractor shall notify the VOA of any possible or potential conflict of interest which may result from other activities, and shall only commence such other activities after obtaining written approval of the VOA which may not be unreasonably withheld.

4.3. The Contractor shall carry out conflict of interest checks on an ongoing basis and take active steps to identify, remove or avoid the cause of any conflict of interest.

4.4. On an on-going basis, the Contractor must declare all private, personal and financial interests and any previous involvement with Property that may pose a potential conflict in respect of the VOA requirements, to the VOA Contract Manager. The Contractor must take all necessary steps to manage or terminate these conflicts.

4.5. The VOA reserves the right to deem any Contractors (and other subcontractors and consortium) party to the same frameworks as the VOA as posing automatic conflicts of interest.

4.6. The VOA reserves the right to take such steps it deems necessary where, in the reasonable opinion of the VOA, there is or may be an actual conflict, or a potential conflict, between the Contractor and the VOA under the provisions of the Contract.

4.7. The actions of the VOA shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the VOA.

5. VOLUME OF WORK

5.1. We cannot guarantee numbers of instructions as part of this contract as they are dependent on instructions from a third party.

5.2. We anticipate volumes of approximately 100 instructions per annum nationally.

4. CONTRACT TERM

The contract term will be for a period of two years (with possible two one year extensions).

5. SUB CONTRACTING

5.1. The supplier shall not assign, novate or otherwise transfer or dispose of any of its rights or obligations under the contract without the prior written consent of the VOA contract manager, which may be withheld at the VOA's absolute discretion, and any attempt by the supplier to assign, novate or otherwise transfer or dispose of its rights or obligations in violation hereof shall be null and void

6. MANAGEMENT INFORMATION

6.1. As a minimum we would expect to be provided with a weekly highlight report summarising progress against agreed milestones, any risks to successful delivery and proposed mitigations, and a financial summary of costs incurred and projected out-turn.

7. VOA CONTRACT MANAGER DETAILS

7.1. The VOA contract manager will be Richard Pugh.

7.2. The VOA reserves the right to appoint an alternative contract manager at any given point throughout the duration of the contract.

7.3. The supplier will be required to appoint a contract manager to serve as the VOA's point of contact within the organisation.

8. PAYMENT TERMS

8.1. Payments will be made via an electronic payments system, SAP Ariba P2P (MYBuy). Invoices should be provided for each milestone within one month of agreement of deliverables and sent to voainvoices.ap@hmrc.gov.uk copying in contract manager email address (including the purchase order provided). Payments will be made

into the bank account provided by the supplier.

TERMS & CONDITIONS

9.1. CCS Framework RM61665 - Lot 1 Built Environment & General Infrastructure – NEC4 PSSC Agreement.

10. TENDER REQUIREMENTS

10.1. Quality Criteria (65%)

10.1.1. Please state whether you have any conflict of interest when taking up this project - mandatory: Pass/ Fail.

10.1.2. Please outline your understanding of the key aims and objectives of this requirement. Your response should demonstrate your understanding and knowledge of the VOA and its business, the requirements context, and your role as the sub-contractor. (Maximum 1 side of A4)

10.1.3. Please explain your approach to managing and delivering the national coverage requirements (Maximum 1 side of A4)

10.1.4. Please explain your approach to identifying and managing risks to meet the short timescales outlined. (Maximum 1 side of A4)

10.1.5. Please include an organogram of your organization.

10.2. Pricing (25%)

For all property types (GIA)	
For the first 100 square metres	
For the next 100 to 500 square metres	
For any area >500 square metres	

Reasonable mileage costs will be payable in addition to the above.

Please provide details of your hourly rates in the event of ad hoc work. These rates will not form part of the scoring.

Role	Building Surveyor
Senior Director	
Director	
Principal / Associate Director	
Senior Professional	
Professional	

Senior Technician	
Technician/Graduate	
Administration	

10.3. Social Value (10%)

This section is for suppliers to describe the commitment their organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria in the table below:

Theme	Policy Outcome	Model Award Criteria	Reporting Metric
Tackling economic inequality	Increase supply chain resilience and capacity	MAC 3.4: Demonstrate collaboration throughout the supply chain, and a fair and responsible approach to working with supply chain partners in delivery of the contract.	Percentage of all companies in the supply chain under the contract to have adopted the National Cyber Security Centre's 10 steps. [where relevant]

Please describe your commitment in the following format:

• Your 'Method Statement', stating how you will achieve this and how your commitment meets the Model Award Criteria

• How you will monitor, measure and report on your commitment/the impact of your proposals.

• How the above will support the Authority's commitments

10.3.2. We recommend that suppliers should look to identify at least 1 key additional reporting metric.

All reporting metrics will be included expressly in the contractual terms.

Examples of suitable reporting metrics may be found in The Social Value Model.

10.3.3. Supplier Social Value response should be a maximum of 500 words. (Text within drawings & graphs is not included in the word count)"

Scope

3. Existing information

List existing information which is relevant to the *service*. This can include documents which the *Consultant* is to further develop

N/A

4. Specifications and standards

List the specifications and standards that apply to the contract.

N/A

Scope

5. Constraints on how the *Consultant* provides the Service

State any constraints on sequence and timing of work and on method and conduct of work including the requirements for any work by the *Client.*

REDACTED is the Supplier's bid response dated 17/05/2023

Scope

6. Requirements for the programme
State whether a programme is required and, if it is, what form it is to be in, what information is to be shown on it, when it is to be submitted and when it is to be updated

N/A

Scope

7. Information and other things provided by the *Client – N/A*
Describe what information and other things the *Client* is to provide and by when. Information is that which is not currently available, but will become available during the contract. Other things could include access to a person, place (such as office space or a site) or the *Client's* information technology systems.

ITEM	DATE BY WHICH IT WILL BE PROVIED

SCHEDULE 1 -**GDPR**

The following definitions shall apply to this Schedule 1

Agreement : this contract;

Processor Personnel : means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation : (i) the GDPR, (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy which, pending a decision from the competent authorities of the EU on the adequacy of the UK data protection regime will include the requirements set out or referenced in Part Three, Title VII, Article 71(1) of the Withdrawal Agreement signed by the UK and the EU in December 2019;

Data Protection Impact Assessment : an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller , Processor , Data Subject , Personal Data , Personal Data Breach , Data Protection Officer take the meaning given in the Data Protection Legislation.

Data Loss Event : any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Request : a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Joint Controllers: where two or more Controllers jointly determine the purposes and means of processing

Protective Measures : appropriate technical and organisational measures which may include: pseudonymisarion and/or encryption of Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [2] (Security).

Sub-processor : any third party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Consultant* is the Processor unless otherwise specified in Schedule

[1]. The only processing that the Processor is authorised to do is listed in Schedule [1] by the Controller and may not be determined by the Processor.

1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 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 operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the *service*;

(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.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule [1], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, 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 Data Loss Event;

(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 this Agreement (and in particular Schedule 1);

(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 clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(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 this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the UK 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 (in accordance with the Data Protection Legislation) 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;

(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 Agreement unless the Processor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject 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 this Agreement;

(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 Data Loss Event.

1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly 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 the Controller to comply with a Data Subject 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 Data Loss Event;

(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.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. 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 GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

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

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

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation .

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 Where the Parties include two or more Joint Controllers as identified in Schedule [X] in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.

ANNEX A - PART 2: SCHEDULE OF PROCESSING,

PERSONAL DATA AND DATA SUBJECTS SCHEDULE [X]

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

This Schedule 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 Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: REDACTED
2. The contact details of the Processor's Data Protection Officer are: REDACTED
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

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

Description	Details
Identity of the Controller and Processor	**REDACTED**

Subject matter of the processing	**REDACTED**
Duration of the processing	**REDACTED**

Type of Personal Data being Processed	**REDACTED**
Categories of Data Subject	**REDACTED**
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	**REDACTED**

SCHEDULE 2

1. CONTRACT SCHEDULE 2 - SECURITY PROVISIONS

1.1 Definitions

For the purposes of this schedule the following terms shall have the meanings given below:

"Affiliates" in relation to a body corporate, any other entity which

directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;

"Breach of Security" in accordance with the Security Requirements and the Security Policy, the occurrence of:

(a) any unauthorised access to or use of the service the Client Premises, the Sites, the Consultant System and/or any ICT, information or data (including the Confidential Information and the Client Data) used by the *Client* and/or the *Consultant* 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 Client Data), including any copies of such information or data, used by the *Client* and/or the *Consultant* in connection with this contract.

"Clearance" means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;

"CONSULTANT EQUIPMENT"

the hardware, computer and telecoms devices and equipment supplied by the *Consultant* or its Subcontractors (but not hired, leased or loaned from the *Client*) for the carrying out of the *service*;

"Consultant Software" software which is proprietary to the *Consultant*, including software which is or will be used by the *Consultant* for the purposes of carrying out of the *service*;

"Consultant System" the information and communications technology system used by the *Consultant* in carrying out of the *service* including the Software, the *Consultant* Equipment and related cabling (but excluding the Client System);

"Control" means that a person possesses, directly or indirectly, the power to direct or cause the direction of the managementand policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;

"Default" any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub Consultants in connection with or in relation to the subject-matter of this contract and in respect of which such party is liable to the other;

"DISPUTE RESOLUTION PROCEDURE"

THE DISPUTE RESOLUTION PROCEDURE SET OUT IN THIS CONTRACT (IF ANY) OR AS AGREED BETWEEN THE PARTIES;

"Client Premises" means premises owned, controlled or occupied by the *Client* or its Affiliates which are made available for use by the *Consultant* or its Subcontractors for carrying out of the *service* (or any of them) on the terms set out in this contract or any separate agreement or licence;

"Client System" the *Client*'s computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the *Client* or the *Consultant* in connection with this contract which is owned by or licensed to the *Client* by a third party and which interfaces with the *Consultant* System or which is necessary for the *Client* to receive the *service*;

"ENVIRONMENTAL INFORMATION REGULATIONS"

the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;

"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;"Good Industry Practice"

THE EXERCISE OF THAT DEGREE OF SKILL, CARE, PRUDENCE, EFFICIENCY, FORESIGHT AND TIMELINESS AS WOULD BE EXPECTED FROM A LEADING COMPANY WITHIN THE RELEVANT INDUSTRY OR BUSINESS SECTOR;

"ICT"	information and communications technology;
"ICT Environment"	the Client System and the *Consultant S*ystem;
"Impact Assessment"	an assessment of a Compensation Event;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;

"INFORMATION ASSETS REGISTER"

THE REGISTER OF INFORMATION ASSETS TO BE CREATED AND MAINTAINED BY THE *CONSULTANT* THROUGHOUT THE CARRYING OUT OF THE *SERVICE* AS DESCRIBED IN THE CONTRACT (IF ANY) OR AS OTHERWISE AGREED BETWEEN THE PARTIES;

"ISMS"	the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the parties and will directly reflect the scope of the *service*;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the *service* but excluding know how already in the *Consultant*'s or the *Client*'s possession before this contract;
"List x"	means, in relation to a Subcontractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub Consultant undertaking work on its premises marked as CONFIDENTIAL or above;

"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Process"	has the meaning given to it under the Data Protection Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;
"Protectively Marked"	shall have the meaning as set out in the Security Policy Framework.
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this contract or any other affairs of the *Client* and "Regulatory Body" shall be construed accordingly;

"REQUEST FOR INFORMATION"

A REQUEST FOR INFORMATION OR AN APPARENT REQUEST UNDER THE CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION, FOIA OR THE ENVIRONMENTAL INFORMATION REGULATIONS;

"SECURITY MANAGEMENT PLAN"

"Security Policy Framework"

"Security Requirements"

the *Consultant*'s security plan prepared pursuant to paragraph 1.5.3 of schedule J (Security Management Plan) an outline of which is set out in Appendix 1 of schedule J (Security Management Plan);

means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);

means the requirements in the contract relating to security of the carrying out of the *service* (if any) or such other requirements as the *Client* may notify to the *Consultant* from time to time

"Security Tests"	shall have the meaning set out in Appendix 2 (Security Management Plan) [Guidance: define “Security Tests” in Security Management Plan]
"Software"	Specially Written Software, *Consultant* Software and Third Party Software;

"SPECIALLY WRITTEN SOFTWARE" any software created by the *Consultant* (or by a third party on behalf of the *Consultant*) specifically for the purposes of this contract;

"Staff Vetting Procedures" the *Client*'s procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;

"Statement of Applicability" shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;

"Standards"	the British or international standards, *Client*'s internal policies and procedures, Government codes of practice and guidance together with any other specified policies or procedures referred to in this contract (if any) or as otherwise agreed by the parties;

"Third Party Software" software which is proprietary to any third party other than an Affiliate of the *Consultant* which is or will be used by the *Consultant* for the purposes of carrying out of the *service.*

1.2 Introduction

1.2.1 This schedule covers:

1.2.1.1 principles of protective security to be applied in carrying out of the *service*;

1.2.1.2 wider aspects of security relating to carrying out of the *service*;

1.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;

1.2.1.4 the creation and maintenance of the Security Management Plan;

1.2.1.5 audit and testing of ISMS compliance with the Security Requirements;

1.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;

1.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

1.3 Principles of Security

1.3.1 The *Consultant* acknowledges that the *Client* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.

1.3.2 The *Consultant* shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

1.3.2.1 is in accordance with Good Industry Practice, the *law of the contract* and this contract;

1.3.2.2 complies with the Security Policy;

1.3.2.3 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) available from the Cabinet Office Security Policy Division (COSPD);

1.3.2.4 meets any specific security threats to the ISMS; and

1.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;

1.3.2.6 complies with the Security Requirements; and

1.3.2.7 complies with the *Client*'s ICT standards.

1.3.3 The references to standards, guidance and policies set out in paragraph 1.3.2.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

1.3.4 In the event of any inconsistency in the provisions of the above standards,

guidance and policies, the *Consultant* gives an early warning to the *Client* of such inconsistency immediately upon becoming aware of the same, and the *Client* shall, as soon as practicable, advise the *Consultant* which provision the *Consultant* shall be required to comply with.

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

(i) The *Consultant* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be accepted, by the *Client*, tested in accordance with the provisions relating to testing as set out in the contract (if any) or as otherwise agreed between the Parties, periodically updated and audited in accordance with ISO/IEC 27001.

1.4.1.1 The *Consultant* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *service*.

1.4.1.2 The *Consultant* shall comply with its obligations set out in the Security Management Plan.

1.4.1.3 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Client*, aim to protect all aspects of the *service* and all processes associated with carrying out of the *service*, including the construction, use, alterations or demolition of the *service*, the *Consultant* System and any ICT, information and data (including the Client Confidential Information and the Client Data) to the extent used by the *Client* or the *Consultant* in connection with this contract.

1.4.2 Development of the Security Management Plan:

1.4.2.1 Within 20 Working Days after the date of this contract and in accordance with paragraph 1.4.4 (Amendment and Revision), the *Consultant* will prepare and deliver to the *Client* for acceptance a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Contract Schedule J.

1.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is accepted by the *Client* it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract Schedule J. If the Security Management Plan is not accepted by the *Client* the *Consultant* shall amend it within 10 Working Days or such other

period as the parties may agree in writing of a notice of non-acceptance from the *Client* and re-submit to the *Client* for accepted. The parties will use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the *Client*. If the *Client* does not accept the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No acceptance to be given by the *Client* pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to accept the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 1.4.3.4 shall be deemed to be reasonable.

1.4.3 Content of the Security Management Plan:

1.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the *Consultant* in relation to all aspects of the *service* and all processes associated with carrying out of the *service* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *service* comply with the provisions of this schedule (including the principles set out in paragraph 1.3);

1.4.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the date of this contract to those incorporated in the *Consultant*'s ISMS at the date notified by the *Client* to the *Consultant* for the *Consultant* to meet the full obligations of the Security Requirements.

1.4.3.3 The Security Management Plan will be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other schedules of this contract which cover specific areas included within that standard.

1.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the *Consultant* and the *Client* engaged in the *service* and shall only reference documents which are in the possession of the *Client* or whose location is otherwise specified in this schedule.

1.4.4 Amendment and Revision of the ISMS and Security Management Plan:

1.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the *Consultant* annually or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Consultant System, the *service* and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by the *Client*.

1.4.4.2 The *Consultant* will provide the *Client* 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 *Client*. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

1.4.4.3 On receipt of the results of such reviews, the *Client* will accept any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.

1.4.4.4 Any change or amendment which the *Consultant* proposes to make to the ISMS or Security Management Plan (as a result of a *Client's* request or change to the *service* or otherwise) shall be subject to the early warning procedure and shall not be implemented until accepted in writing by the *Client*.

1.4.5 Testing

1.4.5.1 The *Consultant* shall conduct Security Tests of the ISMS on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the *Client.*

1.4.5.2 The *Client* shall be entitled to witness the conduct of the Security Tests. The *Consultant* shall provide the *Client* with the results of such tests (in a form accepted by the *Client* in advance) as soon as practicable after completion of each Security Test.

1.4.5.3 Without prejudice to any other right of audit or access granted to the *Client* pursuant to this contract, the *Client* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Consultant*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Consultant*'s compliance with the ISMS and the Security Management Plan. The *Client* may notify the *Consultant* of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the carrying out of the *service*. If such tests adversely affect the *Consultant*'s ability to carry out the *service* in accordance with the Scope, the *Consultant* shall be granted relief against any resultant under-performance for the period of the tests.

1.4.5.4 Where any Security Test carried out pursuant to paragraphs 1.4.5.2 or 1.4.5.3 above reveals any actual or potential Breach of Security, the *Consultant* shall promptly notify the *Client* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Consultant* proposes to make in order to correct such failure or weakness. Subject to the *Client*'s acceptance in accordance with paragraph (i), the *Consultant* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Client* or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is made to address a non-compliance with the Security Policy or Security Requirements, the change to the ISMS or Security Management Plan is Disallowed Cost.

1.5 Compliance with ISO/IEC 27001

1.5.1 Unless otherwise agreed by the parties, the *Consultant* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the date of this contract and shall maintain such certification until the Defects Certificate or a termination certificate has been issued.

1.5.2 In the event that paragraph 1.5.1 above applies, if certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the *Consultant* reasonably believes that it is not compliant with ISO/IEC 27001, the *Consultant* shall promptly notifythe *Client* of this and the *Client* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

1.5.3 The *Client* shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

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

1.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the *Consultant* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Consultant* 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 *Client* in obtaining such audit.

1.6 Breach of Security

1.6.1 Either party shall give an early warning to 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.

1.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 1.6.1, the *Consultant* shall:

1.6.2.1 immediately take all reasonable steps necessary to:

(a) remedy such breach or protect the integrity of the ISMS against any such potential or attempted breach or threat; and

(b) prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably required by the *Client*; and

1.6.2.2 as soon as reasonably practicable provide to the *Client* full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security.