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

Order Form

CALL-OFF REFERENCE: **VOA/2023/012**

THE BUYER: **Valuation Office Agency (VOA)**

BUYER ADDRESS: **10 South Colonnade, London, E14 4PU**

THE SUPPLIER: **Precise Media Monitoring Ltd. (trading as Onclusive)**

SUPPLIER ADDRESS: **222 Grays Inn Road, London, England, WC1X 8HB**

REGISTRATION NUMBER: **03247942**

DUNS NUMBER: **525621686**

SID4GOV ID: **N/A**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 15/08/2023 It's issued under the Framework Contract with the reference number RM6134 for the provision of Media Monitoring and Associated Services.

CALL-OFF LOT(S):
Lot 1

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6134
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6134
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)
        - Joint Schedule 12 (Supply Chain Visibility)

    - Call-Off Schedules for RM6134
        - Call-Off Schedule 1 (Transparency Reports)
        - Call-Off Schedule 2 (Staff Transfer)
        - Call-Off Schedule 3 (Continuous Improvement)
        - Call-Off Schedule 5 (Pricing Details)
        - Call-Off Schedule 6 (ICT Services)
        - Call-Off Schedule 7 (Key Supplier Staff)
        - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
        - Call-Off Schedule 9 (Security)
        - Call-Off Schedule 10 (Exit Management)
        - Call-Off Schedule 14 (Service Levels)
        - Call-Off Schedule 15 (Call-Off Contract Management)
        - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.7)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6134
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:
None.

CALL-OFF START DATE: **28/08/2023**

CALL-OFF EXPIRY DATE: **27/08/2025**

CALL-OFF INITIAL PERIOD: **2 Years**

CALL-OFF DELIVERABLES

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

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 is **£5,705.**

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details) which include the revised pricing proposal and clarifications submitted by The Supplier as part of the tender bid.

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:

- Indexation
- Specific Change in Law

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

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 (and including the purchase order provided). Payments will be made into the bank account provided by the supplier.

BUYER'S INVOICE ADDRESS:
Redacted

BUYER'S AUTHORISED REPRESENTATIVE
Redacted

BUYER'S ENVIRONMENTAL POLICY

Appended at Appendix A

BUYER'S SECURITY POLICY
None in addition to framework requirements.

SUPPLIER'S AUTHORISED REPRESENTATIVE
Redacted

SUPPLIER'S CONTRACT MANAGER
Redacted

PROGRESS REPORT FREQUENCY
Supplier to share progress reports by email to Buyer's Authorised Representative on a monthly basis. Short follow-up calls may be required to discuss points raised in the email.

PROGRESS MEETING FREQUENCY
Quarterly on the first Working Day of each quarter.
Initial contract management meeting to take place before 28th August 2023.
This is separate to the kick-off meeting to take place in week one (1) of Order Start Date.

KEY STAFF
Redacted

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

The Service Credit Cap is: 10% of Quarterly spend
The Service Period is: one Quarter
A Critical Service Level Failure is: observed if any Service is 10% below its Target.

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the following Deliverables and performing its obligations under the Call-Off Contract:

- Not utilise zero hours contracts
- Provide fair pay for workers (Payment of the real Living Wage); Work to attain accreditation by Kantar of 'London Living Wage'
- Not use fire and rehire practices
- Offer and report on flexible and family friendly working practices for all workers from day one of their employment.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

Appendix A – Buyer's Environmental Policy

Environmental Policy

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

The VOA understands the importance of reducing the carbon footprint principally through the use of its estate, using its expertise to demonstrate its commitment to mitigating risk from climate change impacts, through compliance with legislation and regulations, adaptation, and adopting best practice.

The VOA Estates Team adopt an innovative approach to both technology and communication as well as more traditional methods, to encourage awareness of the sustainability policy Agency wide.

Additionally we align our aims and activities alongside our sponsor department HMRC, collaborating with them in our promise to adopt the following
These are as follows:

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

guidance, and to assist in meeting the VOA's environmental sustainability objectives.

This policy will be reviewed and assured at regular intervals.
Customer and stakeholder satisfaction is an essential part of the environmental process, to ensure this is fulfilled the Estates team receive training to ensure awareness and understanding of the environment and its impact of the products or service in which we provide.

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

Joint Schedule 11 (Processing Data)
Schedule 1
Status of the Controller

1. 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. 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 there 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

2. 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.

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

4. 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 Services;

(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.

5. 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*);

(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 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 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.

6. Subject to paragraph 7 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.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

8. 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 6 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.

9. 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 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.

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

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

12. 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.

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

14. The Relevant Authority may, at any time on not less than 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).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 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

16. 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 GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

17. 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.

18. 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.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 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.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

21. 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 GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

24. 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.

25. 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.

26. 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).*

27. 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)*.

28. Notwithstanding the general application of paragraphs 2 to 15 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 paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

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

The contact details of the Relevant Authority's Data Protection Officer are: **Redacted**
1.1
The contact details of the Supplier's Data Protection Officer are: **Redacted**
1.2
1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • **Names and email addresses of the recipients of the daily emails** • **Names and email addresses of those logging into the system**
Duration of the Processing	The duration of the call-off contract.

Nature and purposes of the Processing	*The nature of the Processing means any operation such as collection, recording, structuring, storage, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.*
Type of Personal Data	Names and email addresses
Categories of Data Subject	VOA Staff
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	The Supplier shall ensure that all documents and/or computer records in its possession, custody or control which contain Confidential Information or relate to personal information of the Authorities' employees, ratepayers or service users, are delivered up to the Contract Manager. The Supplier shall ensure that all records listed previously are securely destroyed, 6 months after the contract end.

Annex 2 - Joint Controller Agreement -NOT USED

Call-Off Schedule 4 (Call Off Tender)

Supplier's Bid proposal submitted 27/07/2023

Redacted

Call-Off Schedule 5 (Pricing Details)

PRICING FOR CORE SERVICES (ONLINE, PRESS AND BROADCAST MEDIA MONITORING SERVICES + SUMMARY) SUBMITTED 31/07/2023

Redacted

PRICING FOR ADDITIONAL SERVICES (MEDIA CONTACT DATABASE SERVICE) SUBMITTED 09/08/2023 AND CLARIFIED 10/08/2023.

Redacted

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Annex 1 to this Schedule 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.

Annex 1- Key Roles

Key Role	Key Staff	Contract Details
Redacted	**Redacted**	**Redacted**

Call-Off Schedule 9 (Security)

Part A (Short Form Security Requirements) should apply.

Part A: Short Form Security Requirements

1. Definitions

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

"Breach of Security"	1 the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2 in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

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

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure

that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

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

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

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

4. Security Management Plan

4.1 Introduction

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

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

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

4.3 Development of the Security Management Plan

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

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

4.4 Amendment of the Security Management Plan

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

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

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

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

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

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

5. Security breach

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

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

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

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

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B: Long Form Security Requirements – NOT USED

Baseline security requirements

1. Handling Classified information

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

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the 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 Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the 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 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 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 as per the Buyer's Invitation to Tender – Specification dated 14/07/2023 & the Clarification Q&A Log dated 24/07/23

INVITATION TO TENDER

SPECIFICATION

For the provision of a Framework/Contract to supply

Online, Print and Broadcast Media Monitoring services to the Valuation Office Agency

VOA/2023/012 for the VOA

1. INTRODUCTION

1.1. The Valuation Office Agency (VOA) is an executive agency of her Majesty's Revenue and Customs (HMRC). As the public sector's property valuation experts, we provide valuations and property advice to the government and local authorities in England, Scotland and Wales to support taxation and targeted financial support for families and individuals. The VOA also provide property valuation and surveying services to public sector bodies. Its work includes:

- compiling and maintaining lists of council tax bands for approximately 26 million domestic properties;
- compiling and maintaining lists detailing the rateable value of over 2 million commercial properties for business rates;
- determining Local Housing Allowance rates across England;
- advising local authorities of the maximum subsidy level payable for Housing Benefit claims under the local reference rent system;
- maintaining a register of fair rents for regulated tenancies in England;
- providing statutory valuations to support taxes administered by HMRC and the administration of benefits by the Department for Work and Pensions; and
- providing a range of independent property advice and valuations across the public sector.

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

2. BACKGROUND

2.1. The VOA's External Affairs team is responsible for all proactive and reactive media activity.

2.2. Part of this involves horizon scanning to ensure we are aware of any media interest in particular issues, which helps us to stay ahead of potential problems and avoid reputational damage. And to track coverage of the VOA and share this with internal stakeholders.

3. REQUIREMENT

3.1. The VOA is seeking a media monitoring service which tracks VOA-related coverage. We would like the service to:

- Create and send daily media monitoring reports via email (to an unlimited number of VOA recipients, although in practice this is likely to be limited to fewer than 10 recipients).

- The daily monitoring should include a summary of national news, and a summary and clippings of coverage based on search terms determined by the VOA.
- Recipients should receive clippings no later than 9am (but in practice this is expected to be much earlier in the morning).
- Produce reports according to agreed search terms for up to 100 keywords and search parameters. Requested changes to search terms should be actioned within 2 working days.
- Analyse print (national, regional, local and trade), broadcast (TV and radio) and online (BBC.co.uk, ITV.com etc) news.
- Be compatible with NLA Media Access Licensing services.
- There should be a management portal which hosts all clippings received.

3.2. A supplier will provide a proactive client management function providing regular reporting on how keywords are performing and suggestions for changes, and a designated account manager. This review will help ensure:

- The cuttings we receive will be relevant to our search terms and will keep us within NLA access limits
- Ensure that all relevant media coverage is captured

The supplier should also respond to service-related queries within 48 hours.

3.3. First media clippings to be delivered by 28 August 2023

3.4. There may be demand for ad-hoc services during the contract term, for specific reporting on media coverage, sentiment and favourability, and these will be issued as separate request for quote (RFQ) and agreed by variation.

3.5. Suppliers may be asked to include a Media Contact database service upon award. This is an optional requirement at this stage, and we request pricing information in the pricing template enclosed. It will be evaluated with a minority weighting.

3.6. An awarded supplier will be subject to a compatibility check with the VOA security team, to ensure sites and portals are on our 'whitelist'.

4. MANAGEMENT INFORMATION

4.1. As a minimum we would expect to be able to receive and access information on a monthly basis to help us analyse the coverage received. This will include the volumes of clippings for National, Regional, Foreign, Magazine, Premium Magazine, and Digital Variable Newspapers and Magazines broken down by daily, and weekly volumes, as a minimum.

4.2. Information to help us analyse the relevance of search terms and parameters, including which words/search terms have sourced relevant/irrelevant clippings.

5. TIMETABLE

5.1. Please see below an indicative timetable to outline delivery of the tender.

DATE	ACTIVITY
07/07/2023	Publication of ITT. Clarification period starts.
4pm on 19/07/2023	Clarification period closes ("**Tender Clarifications Deadline**")
4pm on 27/07/2023	Deadline for submission of a Tender to the Authority Contract ("**Tender Submission Deadline**")
07/08/2023	Proposed Award Date of Contract
21/08/2023	Expected commencement date for the Contract

6. CONTRACT TERM

6.1. The contract term will be for a period of 1 years (with a 1 year extension option available).

7. VOA CONTRACT MANAGER DETAILS

7.1. The VOA contract manager will be Portia Gingell.

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.

9. TERMS AND CONDITIONS

9.1. CCS Framework RM6134 - Media Monitoring and Associated Services

10. TENDER REQUIREMENTS

10.1. Quality Criteria (this will form 60% of the evaluation)

10.1.1 Tenderers should outline their understanding of the requirement and their capacity and approach to deliver Section 3 of this Specification – 30%.
Response shall be no more than 750 words.

10.1.2 Proactive account management – 10%.
Tenderers should propose a methodology on how they will provide a quality proactive client management function.
Response shall be no more than 500 words

10.1.3 Tenderers should explain their measures for Quality Control and contingencies for system failure. Responses should include proposals relating to the late/ missed supply of data, or the provision of irrelevant content or content which is surplus to our requirement - 15%.
Response shall be no more than 500 words

10.1.4 Tenderers should outline the features of their Media Contact database services. - 5%
Response shall be no more than 500 words

10.2. Social Value (this will form 10% of the evaluation)

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
Theme 4: Equal opportunity	Policy Outcome: Tackle workforce inequality	**MAC 6.1:** Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce.

10.2.1. 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

Suppliers should look to identify at least 1 key reporting metric in their response.

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

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

Supplier Social Value response should be a maximum of 500 words.

(Text within drawings & graphs is not included in the word count)

10.3. Pricing (This will form 30% of the evaluation)

10.3.1. Tenderers should complete the pricing proposal template attached to the tender invitation email.
Prices will be assessed against the total estimated volumes for each category. As a government agency, price is an important factor and so competitive offers are being sought. Please do not include details of your price in the Quality response – 25%

10.3.2. Pricing for the Media Contact Database service- 5%

11. SCORING

11.1. Scores will be allocated for each quality question in line with the scoring scheme located in Appendix A, and for social value questions in line with the scoring scheme located in Appendix B. The maximum available score will be 100.

11.2. The contract will be awarded to the Tender with the highest combined cost, quality, and Social Value score.

12. TENDER QUERIES

12.1. Tenderers with any queries about the should contact tenders mail to **Redacted** by email before **4pm on 19/07/2023** with the subject title "VOA Print & Broadcast Media Monitoring services Tender Query".

13. TENDER SUBMISSION

13.1. You should send a PDF or read-only electronic copy of your proposal by e-mail to **Redacted**, as an attachment to an e-mail message entitled "VOA Print & Broadcast Media Monitoring services". Tender to arrive **no later than 4pm on 27/07/2023** (unless the date is subsequently amended in writing by the VOA).

13.2. Please note that email messages with this title will not be opened in advance of that deadline. No hard copies of the tender are required.

Appendix A

Score	'Closed' Question Criteria	'Open' Question Criteria
100	Excellent answer which meets all of the requirements and provides all of the required detail.	An excellent response that: • is completely relevant, addressing all of the requirements; • demonstrates an excellent understanding of the requirements, is comprehensive, robust and unambiguous; • provides highly credible supporting evidence, benefits or innovation; and/or • meets the requirements in all aspects, with no ambiguity or weaknesses identified and no clarification required.

80	Good answer which meets all of the requirements but lacks some minor detail	A good response that: • is highly relevant, addressing all of the requirements; • demonstrates a good understanding of the requirements and is comprehensive; • provides supporting evidence of sufficient detail; and/or • meets the requirements in all aspects, but contains minor weaknesses or a small amount of ambiguity.
60	Satisfactory answer, which meets the requirements in many aspects, but fails to provide sufficient detail in some areas.	A satisfactory response that: • is relevant, addressing most or all of the requirements; • demonstrates a satisfactory understanding of the requirements; • provides supporting evidence but lacks detail in some areas; and/or • meets the requirements in most aspects, but contains manageable weaknesses or some ambiguity and may require some
40	Limited answer which satisfies some aspects of the requirements but fails to	A limited response that:
Score	**'Closed' Question Criteria**	**'Open' Question Criteria**
	meet the specification in the whole.	• is mostly relevant, addressing most of the requirements; • demonstrates a limited understanding of the requirements; • provides supporting evidence but lacks detail in some or most areas; and/or • contains weaknesses or ambiguity which suggest that the requirements would not be met unless clarified.

20	Poor answer which significantly fails to meet the requirements.	A poor response that: • is only partially relevant, addressing some of the requirements; • demonstrates a poor understanding of the requirements; • provides supporting evidence that is of limited/insufficient detail or explanation; and/or • contains multiple and/or significant weaknesses or ambiguity that suggest the requirements would not be met.
0	The response is not considered relevant. The response is unconvincing, flawed or otherwise unacceptable. Response fails to demonstrate an understanding of the requirement. No evidence is provided to support the response. Or nil response.	An unacceptable response that: • is not fully relevant, addressing some or none of the requirements; • demonstrates very limited or no understanding of the requirements; • provides little or no supporting evidence that is of insufficient detail or explanation; and/or • is unconvincing, flawed or otherwise inadequate, suggesting that the requirements will not be met. Or nil response.

Appendix B – For Evaluation of Social Value

100	The response is Excellent & Completely Relevant
80	The response is Good & Highly Relevant

60	The response is Satisfactory & Relevant
40	The response is Limited & Partially Relevant
20	The response is Poor & Only Partially Relevant
0	The response is Not Considered Relevant

The Clarification Q&A Log dated 24/07/23:

No.	Question	Answer
1	Could you please indicate an approximate budget allocation by the VOA for the requirements in the ITT?	We do not share the VOA budgets for the project. The specification should be sufficient to determine the requirements and price offer. Please advise if there are any questions to help you understand the requirements.
2	We note in the ITT Specification 4.1 under Management Information that there is a requirement to receive and access information on a monthly basis to help VOA analyse the coverage received. This will include the volumes of clippings for National, Regional, Foreign, Magazine, Premium Magazine, and Digital Variable Newspapers and Magazines broken down by daily, and weekly volumes, as a minimum. To confirm, the VOA would require an analytics platfrm to receive these automated insights?	Our aim here is to be able to track how many clippings we are receiving for each on online, press and broadcast service, and the source of the clipping by type. This could be done either by an analytics platform or a separate/standalone report provided on at quarterly contract management meetings.

3	Please can you indicate the average monthly volumes of coverage across print online and broadcast media? Any insight into the breakdown of volumes across media types would also be beneficial.	Upon receiving and reviewing this Clarification Question, we have reviewed the Price Proposal Template, which will be shared with the Clarification Question & Answer log. Our estimated yearly volumes for Clippings + Summaries are as follows: Online: 600 Print: 2000 Broadcast: 180 Prices will be evaluated using these estimated volumes. These volumes are estimates only, and is not a guarantee of the annual demand volume. As a government agency, price is an important factor and so competitive offers are being sought. We request potential providers to please complete the updated price proposal template titled: VOA Online Print and Broadcast Media Monitoring Services Price Proposal Template - UPDATED
4	In terms of your daily media monitoring reports, which are delivered via email, do you currently receive automated daily media monitoring reports or is there a requirement for human curated daily media monitoring reports?	We are looking to receive clippings that are accurate and relevant to the agreed search terms. We also need an accurate and concise summary of the clippings. We ask that suppliers to explain their capability to do this and propose their approach, this may be automated, or human created or some mixture of both. We would expect there to be an assurance of quality of the relevance of the clippings and the accuracy of the summaries before inclusion in the daily return.
5	ITT 10.2 - Please clarify if this is to do with provider SLA's or Social Commitment within our business.	A mixture of both; we are looking for tenderers to support the VOA's Social Value Policy Outcome of tackling workforce inequality. Tenderers should propose existing or planned measure(s) in addressing inequality in employment, skills and pay in the contract workforce (as per Model Award Criteria) 6.1. At least 1 measure will be treated as a deliverable and be used as an SLA/KPI/Reporting Metric in the contract.

6	ITT 10.2.1 - Please clarify 'Method Statement' and what format is required	Responses should demonstrate an understanding of the Policy Outcome and describe existing or planned measure(s) your organisation is taking, in addressing the Model Award Criteria (MAC) 6.1. Please include in your response how you will implement your measure(s) and how they are relevant to tackling inequality in employment, skills and pay in the contract workforce. Please also include also include an explanation of your proposed measures' impact on delivering MAC 6.1. A minimum of 1 measure will serve as a deliverable within the Call-Off Contract and thus included as an SLA/KPI. Therefore, we ask tenderers to propose how they will monitor, measure and report on their measure. The Social Value Model linked below contains illustrative examples of which tenderers may choose to include: https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts A written response is sufficient, with a maximum of 500 words. Tenderers may add use graphics, drawings or graphs if relevant.