**DPS FRAMEWORK SCHEDULE 4: LETTER OF APPOINTMENT AND CONTRACT TERMS**

* 1. **Letter of Appointment**

Demos

REDACTED

Dear Mr REDACTED

**Letter of Appointment**

**CCZZ20A42 - Collective Intelligence Tool to collate public and cross-government insights, and capture diversity of thought.**

This letter of Appointment dated 22nd September 2020, is issued in accordance with the provisions of the DPS Agreement (RM6018) between CCS and the Supplier.

Capitalised terms and expressions used in this letter have the same meanings as in the Contract Terms unless the context otherwise requires.

|  |  |
| --- | --- |
| Order Number: | To be confirmed |
| From: | **National Security Secretariat Embed, Policy Lab** ("Customer") |
| To: | Demos ("Supplier") |

|  |  |
| --- | --- |
| Effective Date: | The Contract will commence on the 28th September 2020 on the proviso that you have the Security Clearance in place by the Contract commencement date. If not the Contract will commence once the security elements are in place |
| Expiry Date: | End date of Initial Period: Twelve weeks after the commencement date of the contracts  End date of Maximum Extension Period: Not Applicable  Minimum written notice to Supplier in respect of extension: Not Applicable |

|  |  |
| --- | --- |
| Services required: | Set out in Section 2, Part B (Specification) of the DPS Agreement and refined by:  · the Customer’s Project Specification attached at Annex A and the Supplier’s Proposal attached at Annex B; and |

|  |  |
| --- | --- |
| Key Individuals: | REDACTED National Security Innovation and Engagement Lead Cabinet Office  Email address REDACTED  Telephone REDACTED  Demos  REDACTED  Director of CASM  REDACTED |
| [Guarantor(s)] | Not Applicable |

|  |  |
| --- | --- |
| Contract Charges (including any applicable discount(s), but excluding VAT): | Total Value of the Contract £67,905.00 (excluding VAT) |
| Insurance Requirements | Additional public liability insurance to cover all risks in the performance of the Contract, with a minimum limit of £1 million for each individual claim  Additional employers' liability insurance with a minimum limit of £1 indemnity  Additional professional indemnity insurance adequate to cover all risks in the performance of the Contract with a minimum limit of indemnity of £1 million for each individual claim.  Product liability insurance cover all risks in the provision of Deliverables under the Contract, with a minimum limit of £1 million for each individual claim |
| Liability Requirements | **Suppliers limitation of Liability** (Clause 18 of the Contract Terms); |
| Customer billing address for invoicing: | Invoices should be submitted to:APinvoices-CAB-U@gov.sscl.com |

|  |  |
| --- | --- |
| GDPR | Contract Terms Schedule 7 (Processing, Personal Data and Data Subjects] |
| Alternative and/or additional provisions (including Schedule 8(Additional clauses)): | See Terms & Conditions Schedule 8 |

**FORMATION OF CONTRACT**

**BY SIGNING AND RETURNING THIS LETTER OF APPOINTMENT (which may be done by electronic means) the Supplier agrees to enter a Contract with the Customer to provide the Services in accordance with the terms of this letter and the Contract Terms.**

**The Parties hereby acknowledge and agree that they have read this letter and the Contract Terms.**

**The Parties hereby acknowledge and agree that this Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of this letter from the Supplier within two (2) Working Days from such receipt**

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

Name and Title: Name and Title:

REDACTED REDACTED

Director, CASM Senior Finance Business Partner

Signature: Signature:

REDACTED

REDACTED

Date: 30th September 2020 Date: 07th October 2020

**Annex A**

**Customer Project Specification**

# SCOPE OF REQUIREMENT

## This experimental twelve (12) week project must include:

## The utilisation of a COIN tool (if the COIN tool is digital, this must include the provision, installation and administration of the COIN tool);

## Collaboration with government to establish topics and/or questions to feed into the COIN;

## A weekly report on COIN analysis; and,

## Provision of a report summarising the findings from the COIN debate, as well as options for a long term COIN capability.

# The requirement

## The COIN must be easily accessible to the target audiences, and consist of three sub-COINS or groups:

## 

## 

## The Supplier must be responsible for maintaining roughly consistent levels of engagement with the three target groups:

## Group 1a - The public - engage with British citizens at home and abroad, so that we might identify novel ideas and solutions based on their lived experience;

## Group 1b - The public - those from anywhere in the world with whom we may wish to engage due to their relevant skills or experience that allow them to challenge and generate innovative ideas. This could include academics and divergent thinkers; and

## Group 2 - Within government - to conduct peer challenge and generate novel solutions.

* 1. The responses must come from a diverse sample within each target group, and not concentrated within a narrow subset of departments/organisations, regions or demographics.

## Group 1a and 1b are not mutually exclusive - an individual could easily fit into both groups. Group 2 will operate in a classified environment, and thus must be separate from group 1. However, it is important that these two groups meaningfully interact with the group 2 COIN, and vice versa. The objectives will be to:

## Benefit policy- and strategy-making, including by harnessing diverse inputs; identifying innovative solutions or alternatives; identifying lessons;

## Improve HMG engagement with stakeholder groups and the public, including by having a positive impact on HMG’s understanding of citizens’ lived experiences; and

## Help evaluate whether HMG should invest in further developing COIN capability.

## Any proposed products must be able to demonstrate how a debate has evolved throughout its duration, and allow participants the opportunity to build on each other's strengths, skills, experience and diversity of thought, thereby maximising the COIN’s collective intelligence.

## It must not be possible to assign contributions to individuals. The product should collect demographic data on an opt-in basis from public participants, and department and profession data from government participants on a compulsory basis. The Supplier must draft participant terms and conditions for agreement by CO prior to the product launch. Participants’ feedback must be collected in weeks 10-11 of the project as the COIN exercise draws to a close. This feedback should be summarised in the final report.

## The Supplier must adhere to the timescales outlined in paragraph 7, except where deviation is confirmed acceptable in writing with CO. The Supplier must participate in the project governance and management outlined in paragraphs 7 and 8.

## The Supplier may proposed digital or non-digital COIN tools as part of their proposal.

## Should the Supplier propose a digital COIN tool, the COIN tool must be hosted on CO infrastructure. All contracted staff must possess Security Check (SC) clearance, or, if not in possession, successfully pass that vetting, prior to commencing the project. See paragraph 16 for further information. The Supplier must specify how many individuals from the contracted organisation would be working on this project.

## The Supplier must provide two final reports:

## Report 1 for participants (content to be confirmed with CO); and,

## Report 2 for CO, including analysis of COIN debates, lessons learned, and options for a long-term COIN capability.

## The Supplier must design an interface for the COIN that is accessible for all demographics for the groups. This must be submitted to CO for their review and approval before using in the launch.

## The Supplier must have due regard for ethical considerations during this project, including:

## The Supplier must confirm their General Data Protection Regulations compliance.

## The Supplier must exercise independent professional judgement in the design, conduct and reporting of their professional activities.

## The Supplier must strive to operate within the constraints of the law (originating country, local law and maybe even international law) on how data on private individuals are to be held, managed and, if required by law, disclosed to the appropriate authorities.

## The Supplier must ensure that participation in their activities is based on voluntary informed and unambiguous consent and that this consent may be retracted at any time by the participants.

## The Supplier must respect the confidentiality of information collected in their professional activities.

## The Supplier must be transparent as to the subject and purpose of data collection.

## The Supplier must ensure that participants are not harmed or adversely affected by their professional activities.

## The Supplier must balance the needs of participants and their activities.

## The Supplier must be straightforward and honest in all their professional relationships.

## The Supplier must respect the rights and well-being of all individuals.

## The Supplier must inform CO of any cases of relevant criminal activities, exploitation, or self-harm as soon as possible, but no later than within one working day of being aware of this information.

## The Supplier must report any conflict of interest or other issues impacting the project to CO.

# Key milestones and Deliverables

## The following Key Milestones/Deliverables will apply for the Contract:

|  |  |  |
| --- | --- | --- |
| e | Description | Timeframe or Delivery Date |
| 1 | Supplier personnel to demonstrate valid SC clearance or undergo SC clearance process | Within one working day of contract award. |
| 2 | Initiate the project | Within one week of SC vetting awarded. |
| 2 | Submit project initiation document, initial risk assessment | By the end of week 1 after project initiation |
| 3 | Progress meetings | Weekly from weeks 1-10 |
| 4 | Agree with CO topics to be input into the tool | By the end of week 1 after project initiation |
| 5 | Agree participant terms and conditions with CO | By the end of week 1 after project initiation |
| 6 | Install and test capability on CO infrastructure | By the end of week 2 after project initiation |
| 7 | Recruit COIN participants | By the end of week 2 after project initiation |
| 8 | Submit updated risk assessment, reflecting improved understanding of project risks | By the end of week 2 after project initiation |
| 9 | First meeting with Senior Responsible Officer (SRO) | By the end of week 2 after project initiation |
| 10 | Launch the COIN | On the Monday of week 3 after project initiation |
| 11 | Interim meeting with SRO presenting interim findings | By the end of week 6 after project initiation |
| 12 | COIN draws to a close. Obtain participant feedback. | By the end of week 10 after project initiation |
| 13 | Delivery of two final reports:For participants (content to be confirmed with CO); and,For CO, including analysis of COIN debates, lessons learned, and options for a long-term COIN capability. | By the end of week 12 after project initiation |
| 14 | Final meeting with SRO, including presentation of final report findings. | By the end of week 12 after project initiation |

# 

# MANAGEMENT INFORMATION/reporting

* 1. The Supplier must provide a project initiation document for CO approval, which must detail:
     1. Project Goals;
     2. Scope;
     3. Stakeholders;
     4. Risk owner(s) within the Supplier’s organisation;
     5. Risks (things that require active mitigations or controls);
     6. Issues (things to monitor, but not actively control); and
     7. Reporting frameworks.
  2. The CO team will nominate a named day-to-day point of contact for the supplier, with whom the Supplier will meet for 30 minutes weekly (likely over videoconference or other mutually agreed remote means during the Covid-19 response) for a progress meeting for weeks 1-10 of the project. A weekly report, summarizing work since the last progress meeting must be sent one working day prior to each progress meeting, which must cover:
     1. Statistics on the overall number of contributors and contributions over the past week, including week-on-week comparisons;
     2. Summary analysis of how the debate has evolved over the past week, including emerging trends and sentiment;
     3. Progress against milestones; and
     4. Updates on the project risk assessment including whether controls are proving satisfactory, and an opportunity to raise any new emerging risks.
  3. The agenda of the meeting will be roughly a fifteen (15) minute presentation from the Supplier and fifteen (15) minutes of questions from CO. The Supplier must provide a short written summary of discussion, actions and any lessons identified, within one working day for comment and agreement by CO.
  4. CO must also provide a named SRO, with whom the Supplier will meet during weeks 2, 6 and 12 (as outlined in paragraph 3) for a sixty (60) minute meeting. During weeks 2 and 6, the SRO meeting will replace the weekly progress meeting. The meeting must follow a similar format to the weekly progress meetings, but must provide more detail with roughly thirty (30) minutes of presentation and thirty (30) minutes of questions. Importantly, the Supplier must detail how the products and services meet the agreed quality acceptance criteria at the SRO meeting.

# volumes

* 1. The volumes have been have been outlined in Section 2 – The Requirement.

# continuous improvement

## The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

## The Supplier should present new ways of working to the CO team during monthly Contract review meetings.

## Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

## The CO and supplier teams must jointly record lessons learned throughout the duration of the project, as outlined in paragraph 4.

# SUSTAINABILITY

* 1. There are three options for the sustainability of the project:
     1. Extend the experiment on the same subject, or a further experiment on an alternative subject;
     2. Work towards a mainstream capability by scaling up the service; or
     3. Discontinue the experiment.

# QUALITY

* 1. Data visualisations must follow best practice on the appropriate use of colour schemes and formatting. Their design must follow inclusive design principles, prioritising accessibility and usability, including the use of alt-text. The content must ideally be accessible for users aided by common assistive technologies, adhering to [Web Content Accessibility Guidelines 2.1](https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag) level AA. However, as this project is akin to a public beta this is not essential.
  2. The user interface must be straightforward and intuitive for users to navigate. This will be pre-agreed with CO during meetings.
  3. The system must be reliably available for users to interact with throughout the day, with any down-time scheduled for times when users are less likely to be active, with users notified in advance.
  4. The service and system must be designed to encourage and facilitate constructive debate among users, who are working towards an agreed position on a given topic.
  5. Necessarily data validation must be conducted. For example, needed checks that those assigned to COIN network 1b, “Public with relevant skills and experience”, meet the agreed requirements for this.
  6. Once the contract is awarded, the first step must be to clarify acceptance criteria based on the specified tool to be used.

## The Supplier **must** adhere to the following essential technical standards:

## The Service Standard;

## The Technology Code of Practice;

## HMG Security Policy Framework;

## Cyber Essentials;

## Web Content Accessibility Guidelines (WCAG) 2.1 AA or its European equivalent EN 301 549;

## Equality Act 2010, section 20 (“reasonable adjustments”) and section 149 (“public sector equality duty”);

## General Data Protection Regulations (GDPR) 2018;

## Privacy and Electronic Communications Regulations (PECR) 2003;

## Public Contract Regulations 2015; and

## The Public Sector Bodies Accessibility Regulations (PSBAR) 2018.

## Additionally, ISO 27001:2013 is desirable.

# PRICE

9.1 The price paid to the Supplier will be a fixed fee. This fee is to cover any initial set-up costs for a period of eight weeks with two weeks either side for project ~~start~~ initiation and conclusion, as outlined in paragraph 7.   
Developing and testing the initial questions to frame the debate;

## Moderating and overseeing the process during the deliberation;

## Weekly production of a short, visual report detailing the outcomes of the deliberation, including descriptions of groups and areas of consensus and disagreement;

## Attending the weekly catch-ups and monthly contract meeting with the CO team;

## A number of days, possibly on-site, for technical support to CO staff to assist them in;

## Setting up, testing under load and maintaining the tool for duration of the consultation;

## Liaising with CO compliance to ensure data is secured sufficiently securely to meet IT requirements;

## Monitoring servers to ensure sufficient provisioning during discussions (and prevent overprovisioning); and

## Implementing tweaks or additions to functionality where necessary.

## If agreed, each additional month of data collection will be priced at a fixed monthly fee.

# STAFF AND CUSTOMER SERVICE

## The Supplier must provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

## The Supplier staff assigned to the Contract must have the relevant qualifications and experience to deliver the Contract to the required standard.

## The Supplier must ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

* 1. The Supplier must maintain a regular, named point of contact with the CO team, who is available within normal business hours to answer queries.
  2. The Supplier must have a track record of successfully delivering projects in the IT and data science space. It is preferred that supplier team members also have experience in developing COINs and/or in conducting public polls.

# SERVICE LEVELS AND CUSTOMER SERVICE

* 1. The Supplier must be assessed against their capacity for building a tool which encourages productive debate and progress towards agreed positions among the COINs. This is the primary objective, to facilitate respondents moving from a position of disagreement on challenging issues to one of agreement through debate and discussion.

|  |  |  |  |
| --- | --- | --- | --- |
| KPI | Service Area | KPI/SLA description | Target |
| 1 | Target group: British citizens | Total number of respondents (i.e. those providing at least one point of data) within 2 months of going live. | 1,000 minimum |
| 2 | Target group: British citizens | Number of question responses (including qualitative and quantitative) received. | 8,000 per month |
| 3 | Target group: UK public | Responses should be weighted by the supplier according to age, gender, religion and region. | Weights applied to sample groups should not be higher than 4 or less than 1. |
| 4 | Target group: Civil Servants | Total number of respondents (i.e. those providing at least one point of data) within two months of going live. | 500 minimum |
| 5 | Target group: Civil Servants | Number of question responses (including qualitative and quantitative) received. | 4,000 per month |
| 6 | Target group: Public with relevant skills and experience | Total number of respondents (i.e. those providing at least one point of data) within 2 months of going live. | 200 minimum |
| 7 | Target group: Public with relevant skills and experience | Number of question responses (including qualitative and quantitative) received. | 2,000 per month minimum |
| 8 | Correspondence | Responding to inquiries from the Contracting Authority. | Within one working day. |
| 9 | Technical fixes | Execution of risk mitigations and technical fixes. | Within one working day. |
| 10 | Moderation | Moderation of public-facing networks. | Ensure no offensive contributions are published, and that the lag between the receipt of contributions and publication created by moderation is no more than one working day. |
| 11 | Technical standards | Adherence to the technical standards outlined in paragraph 6. | No compromise of these standards. |
| 12 | Technical or service incident reporting. | Timely notification of any incidents. | Within one working day. |
| 13 | Data protection | Compliance with the GDPR, and data security. | No data security breaches take place. |

# SECURITY AND CONFIDENTIALITY REQUIREMENTS

* 1. The product must be based on CO servers. The internal network must be classified at OFFICIAL-SENSITIVE, while the external network must be OFFICIAL.
  2. **Secure Configuration**
     1. A Security Configuration Document (SCD) must be supplied by the Buyer upon installation of any digital tools and the measures must be implemented by the Supplier.
  3. **Certification Requirements**
     1. The Supplier and any third party Subcontractors must hold either Cyber Essentials certification. ISO 27001:2013 certification is desirable.
  4. The Supplier must perform a technical information risk assessment on the service supplied and must be able to demonstrate what controls are in place to address those risks.
  5. **End User Device**
     1. The Supplier must ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted.
  6. The Supplier must ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the [NCSC End User Devices Platform Security Guidance](https://www.ncsc.gov.uk/guidance/end-user-device-security).
  7. **Testing**
     1. The Supplier must at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.
  8. **Networking**
     1. The Supplier must ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted when transmitted.
  9. **Personnel Security**
     1. All Supplier Personnel must be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. All Supplier staff must be required to undergo SC vetting.
  10. **Identity, Authentication and Access Control**
      1. The supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The supplier must retain records of access to the physical sites and to the service. These controls must be agreed with the Buyer.
  11. **Data Destruction/Deletion**
      1. The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on, in accordance with the timescales as set out by the Authority/Buyer.
  12. **Audit and Protective Monitoring**
      1. The Supplier must collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records must (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.
  13. **Location of Authority/Buyer Data**
      1. The Supplier must not, procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier must not change where it or any of its Subcontractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.
  14. **Vulnerabilities and Corrective Action**
      1. Suppliers must procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.
  15. Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.
  16. **Incident reporting**
      1. Any security incidents must be reported to the buyer within 24 hours.
  17. **Secure Architecture**
      1. Suppliers must design the service in accordance with:
      2. The NCSC [Security Design Principles for Digital Services](https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main);
      3. The [NCSC Bulk Data Principles;](https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main) and,
      4. The NCSC [Cloud Security Principles](https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles).
  18. Information regarding this project should not be shared outside of the government and the contracted organisation team who are working on this project. Exceptions can be made with explicit permission from the CO team.

# PAYMENT AND INVOICING

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

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

## Invoices must be submitted to: APinvoices-CAB-U@gov.sscl.com

# CONTRACT MANAGEMENT

## Attendance at Contract Review meetings must be at the Supplier’s own expense.

## The supplier will meet with government representatives weekly for a minimum of thirty (30) minutes, as well as SRO meetings at weeks 2, 6 and 12 (likely over videoconference or other mutually agreed remote means during the Covid-19 response).

# Location

## Services will be carried out offsite at the Suppliers site.

## Onsite visits may be necessary to host the tool on CO servers, for which the Supplier will need to be escorted.

**Annex B**

**Supplier Proposal**

REDACTED

.

**ANNEX C PRICING SCHEDULE**

REDACTED