DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	itt_87526
THE BUYER:	Department for Science, Innovation and Technology
BUYER ADDRESS	100 Parliament Street, London, SW1A 2AU
THE SUPPLIER:	Rand Europe
SUPPLIER ADDRESS:	Eastbrook, Shaftesbury Road, Cambridge, CB2 8BF
REGISTRATION NUMBER:	599625179
DUNS NUMBER:	345813547

DPS SUPPLIER REGISTRATION SERVICE ID: 1035631

This Order Form is for the provision of the Deliverables and dated 05/12/2025.
It's issued under the DPS Contract with the reference number RM6200 for the provision of Monitoring AI Adoption and Risks in Critical National Infrastructure.

DPS FILTER CATEGORY(IES):
End-to-End Partnerships, Virtual Assistants and Chatbots, Blue Light, Central Government, Devolved, Administrations, Health, Local Government, Not-for-profit

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order 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 Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6200.
3. The following Schedules in equal order of precedence:
   - Joint Schedules for RM6200:
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information)
     - Joint Schedule 6 (Key Subcontractors)
     - Joint Schedule 7 (Financial Difficulties)
     - Joint Schedule 10 (Rectification Plan)

- Joint Schedule 11 (Processing Data)
- Joint Schedule 12 (Supply Chain Visibility)

● Order Schedules for RM6200:

Order Schedule 1 (Transparency Reports)
Order Schedule 2 (Staff Transfer)
Order Schedule 3 (Continuous Improvement)
Order Schedule 5 (Pricing Details)
Order Schedule 8 (Business Continuity and Disaster Recovery)
Order Schedule 9 (Security)
Order Schedule 10 (Exit Management)
Order Schedule 20 (Order Specification)

4. CCS Core Terms (DPS version) v1.0.1
5. Joint Schedule 5 (Corporate Social Responsibility) RM6200.
6. Order Schedule 4 (Order Tender)
7. Annex 1 – DSIT DESNZ & DSIT Environmental Policy

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

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:

ORDER START DATE: 05/01/2026

ORDER EXPIRY DATE: 05/07/2026

ORDER INITIAL PERIOD: 6 months

DELIVERABLES
See details in Order Schedule 20 (Order Specification)

MAXIMUM LIABILITY
The limitation of liability for this Order 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 <Redacted under s43 of the FOIA>.

ORDER CHARGES
See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
N/A

PAYMENT METHOD
BACS

BUYER'S INVOICE ADDRESS:
<Redacted under s40 of the FOIA>

BUYER'S AUTHORISED REPRESENTATIVE
<Redacted under s40 of the FOIA>

<Redacted under s40 of the FOIA>

BUYER'S ENVIRONMENTAL POLICY
See Annex A - DESNZ & DSIT Environmental Policy v1.5 (1)

BUYER'S SECURITY POLICY
Government security - GOV.UK (www.gov.uk)

SUPPLIER'S AUTHORISED REPRESENTATIVE
<Redacted under s40 of the FOIA>

SUPPLIER'S CONTRACT MANAGER
<Redacted under s40 of the FOIA>

PROGRESS REPORT FREQUENCY
TBC at kick off meeting

PROGRESS MEETING FREQUENCY
TBC at kick off meeting

KEY SUBCONTRACTOR(S)
N/A

E-AUCTIONS
N/A

COMMERCIALLY SENSITIVE INFORMATION
See Joint Schedule 4

SERVICE CREDITS
N/A

ADDITIONAL INSURANCES
N/A

GUARANTEE
N/A

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)

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

Date:		Date:	

Joint Schedule 1 (Definitions)

DPS Joint Schedule 1 - Definitions v.1.0.pdf

Joint Schedule 2 (Variation Form)

DPS Joint Schedule 2 - Variation Form v1.0.

Joint Schedule 3 (Insurance Requirements)

DPS Joint Schedule 3 - Insurance Requirem

Joint Schedule 4 (Commercially Sensitive Information)

1. **What is the Commercially Sensitive Information?**

In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Item(s)	Duration of Confidentiality
1	Technical Bid	The Contract
2	Cost Breakdown	The Contract
3	Contact name and details	The Contract

Joint Schedule 6 (Key Subcontractors)

DPS Joint Schedule 6
- Key Subcontractors

Joint Schedule 7 (Financial Difficulties)

DPS Joint Schedule 7 - Financial Difficulties

Joint Schedule 10 (Rectification Plan)

DPS Joint Schedule 10 - Rectification Plan

Joint Schedule 11 (Processing Data)

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that DSIT:

a. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
b. shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
c. is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
d. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
e. shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. **Undertakings of both Parties**

1. The Supplier and the Relevant Authority each undertake that they shall:

a. report to the other Party every 2 months on:

i. the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
ii. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
iii. any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
iv. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
v. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

b. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

c. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
d. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
e. request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
f. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
g. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
i. are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
ii. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
iii. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
h. ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
i. nature of the data to be protected;
ii. harm that might result from a Personal Data Breach;
iii. state of technological development; and
iv. cost of implementing any measures;
i. ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
j. ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2. Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. **Data Protection Breach**

1. Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any

Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

a. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
b. all reasonable assistance, including:

i. co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
ii. co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
iii. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
iv. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

2. Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

a. the nature of the Personal Data Breach;
b. the nature of Personal Data affected;
c. the categories and number of Data Subjects concerned;
d. the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
e. measures taken or proposed to be taken to address the Personal Data Breach; and
f. describe the likely consequences of the Personal Data Breach.

4. **Audit**

1. The Supplier shall permit:

a. the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
b. the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

2. The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

1. The Parties shall:

a. provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

b. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. **Liabilities for Data Protection Breach**

If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

a. if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

b. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

c. if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

1. If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data

Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

a. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

b. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

c. if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

3. Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. **Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. **Sub-Processing**

1. In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

a. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

b. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Joint Schedule 12 (Supply Chain Visibility)

DPS Joint Schedule 12 (Supply Chain Visil

Order Schedule 1 (Transparency Reports)

DPS Order Schedule 1 - Transparency Rep

Order Schedule 2 (Staff Transfer)

DPS Order Schedule 2 - Staff Transfer v1.0

Order Schedule 3 (Continuous Improvement)

DPS Order Schedule 3 - Continuous Impro

Order Schedule 4 (Order Tender)

<Redacted under s40 of the FOIA>

Order Schedule 5 (Pricing Details)

<Redacted under s43 of the FOIA>.

Pricing Schedule for RAND CNI Monitoring Contract

Deliverable Due	Deliverable	Deliverable Description	Payment Amount
30/01/2026	**D1 – Finalised Project Schedule**	**Final project schedule shared for AISI approval, including baseline risk register.**	<Redacted under s43 of the FOIA>.
09/02/2026	**D2 - CNI-Wide Landscape Mapping**	**High-level landscape map of AI adoption and risks across CNI, including a prioritised list of risk themes to guide sectoral deep dives.**	<Redacted under s43 of the FOIA>.
30/03/2026	**D3 – Draft Frameworks for Energy and Water Sector Deep Dives**	**Draft sector-specific risk monitoring frameworks, including sector-specific fragility profiles and draft monitoring indicators.**	<Redacted under s43 of the FOIA>.
25/05/2026	**D4 – Draft Framework and Indicator Design**	**Draft cross-sector risk monitoring framework, including indicators and data collection methods.**	<Redacted under s43 of the FOIA>.
29/06/2026	**D5 – Finalised Framework and Toolkit**	**Cross-sector risk monitoring toolkit, including the tested and validated AI risk monitoring framework, pilot protocol, guidance materials, and briefing documents to support end-user adoption and expansion.**	<Redacted under s43 of the FOIA>.
			<Redacted under s43 of the FOIA>.

Order Schedule 8 (Business Continuity and Disaster Recovery)

DPS Order Schedule 8 - Business Continuit

Order Schedule 9 (Security)

DPS Order Schedule 9 - Security v1.0.pdf

Order Schedule 10 (Exit Management)

DPS Order Schedule 10 - Exit Management

Order Schedule 20 (Order Specification)

1. Introduction

The UK AI Security Institute (AISI) is working to understand, monitor, and mitigate emerging risks stemming from the integration of advanced AI systems into Critical National Infrastructure (CNI) sectors. As part of this, DSIT is procuring external partners to map adoption of AI by sectors and develop methodologies to monitor risks in order to support preparedness efforts by government departments, key regulators, and other relevant stakeholders.

2. Requirements

The Supplier must develop and validate practical and actionable methodologies for monitoring complex risks arising from the integration of advanced AI into CNI sectors for postdelivery uptake by government departments, key regulators and sector-specific risk owners. In particular, the Supplier must provide a:

1. Clear mapping of AI adoption across CNI sectors and preferably critical supply chains. This should include a breakdown of types of AI applications and tools in use and for what tasks, and current rates of adoption across different kinds of tools and use cases. Ideally the Supplier would also provide a mapping of the market of AI application and tool providers.
2. Analysis of pathways to risk from AI integration into CNI sectors.
3. Robust and practical methodologies for monitoring risks from AI integration into CNI sectors. These methodologies should be usable both across and within specific sectors and should be developed with end-users in mind.

3. Proposed Methodology

The Supplier must recommend a methodology in line with the requirements and specifications of the Technical Submission.

The methodology, core milestones, and KPIs will be agreed with the Buyer based on the tender submission. The Buyer would provide verbal and/or written feedback to refine this proposal at the project inception meeting, and the supplier would be expected to make the necessary changes and then provide a written copy of the updated plan for any further feedback. Following the project kick-off, the Buyer expects monthly progress meetings with the Supplier and regular project updates that raise delivery risks where necessary.

Whilst the project methodologies should be proposed by the Supplier as part of their bid, the Buyer expects the following:

- The Supplier must adopt a mixed-method approach, integrating both qualitative and quantitative insights to inform findings and deliverables.
- The Supplier must involve end-users (e.g., sector regulators) in the design and validation of its methodologies to ensure postdelivery uptake.
- The Supplier must ensure that deliverables are not duplicative or in conflict with existing risk management frameworks or guidelines in CNI.
- Maximum timeframe of 6 months.

4. Governance and Working Arrangements

The Supplier must confirm a named point of contact through whom all enquiries can be filtered. Key Supplier Staff (Order Schedule 2) will be identified in the Tenderer's response.

A project manager from the Buyer will be assigned to the project and will be the central point of contact for the Supplier. The project manager will be available to answer queries and support development regularly, at least at a frequency of once every two weeks. This can be assessed with the Supplier if greater frequency is required, for example towards the end of the project. Project management meetings will be held by either video conference or telephone.

The project manager, the Research Lead, and the SRO of the Buyer's team from which this funding comes, will be responsible for signing off the final outputs of the research project.

The Supplier will review DPS Order Schedule 8 (Business Continuity & Disaster Recover) and develop a high level but proportional plan satisfying this Schedule's requirements in the first 30 days of the Contract. The Buyer will be required to review this plan, but emphasis is given that the plan *must be proportional* to the Schedule's requirements and should not exceed 4 pages of A4.

The Supplier will review DPS Order Schedule 9 (Exit Management) and develop a high level but proportional plan satisfying this Schedule's requirements in the first 30 days of the Contract. The Buyer will be required to review this plan, but emphasis is given that the plan *must be proportional* to the Schedule's requirements and should not exceed 2 pages of A4.

5. Service Levels and Performance

DSIT will measure the quality of the Supplier's delivery by:

- Ability to respond to all queries within 2 working days. For example, responding to emails, providing project updates and providing ad-hoc data and project information.
- Open and engaged communication through the development of the research and discovering of findings.
- The quality of the Supplier's delivery against achievements of key milestones. Milestones dates are indicative and will be agreed between DSIT and the Supplier during project initiation.
- These key milestones are material to the Contract and on-time delivery is of the essence.

6. Risks

The Supplier is required to identify and assess the risks associated with undertaking the research and propose how these may be managed and overcome. The Supplier will develop and manage a full risk register. These should be reported in weekly updates and reviewed at bi-weekly meetings with DSIT.

It is important to note a key risk that we are aware of is the short delivery timelines. We are keen that Suppliers can establish an effective approach to timely delivery.

7. Ownership and Publication

The Buyer will own the intellectual property of all deliverables. The Supplier should prepare the deliverables for the outputs in both publishable (redacted) and not-to-be-published (unredacted) formats. The Supplier will agree the approach to redactions in reviewing near-final drafts and consider this as part of the sign-off process for the final outputs.
The Buyer reserves the right to make the final decision about whether and how to publish the outputs, in line with internal protocols on publication approvals, publication template, branding, accessibility, publication location, and communications handling advice. All published deliverables should be in English and in a clear and accessible language.

The Buyer will be authorised to reproduce products and information in internal and external documents (including those shared with other Government Departments) with the source of information attributed to the Supplier.

8. Quality Management

The Supplier should have measures in place to ensure that the deliverables produced are of a high quality and free from error. Quality assurance measures should be factored into workplan timelines. The quality assurance plan must consider and include as minimum standards those measures detailed in the Government Social Research Code, The Green Book and The Magenta Book where appropriate.

The Supplier will be required to undertake appropriate, independent quality assurance of all deliverables and guarantee the accuracy of all outputs to the Buyer. This could for example be carried out by an external academic.
The Supplier will be required to provide details of the quality assurance procedures they have in place in their bid. During the project, it will also be required to detail what quality assurance processes they have undertaken during the research.

9. Social Value

In addition to the aims, objectives and outcomes of the project, all UK Government contracts are required to contribute to wider social value as an additional benefit of the contract. Social value is a broad term used to describe the wider social, environmental and economic effects of an organisation's actions, and how they contribute to the long-term wellbeing of individuals, communities and societies. More detail can be found here.

Social value is not just a policy requirement. Social value directly supports the mission of DSIT. We require the selected Supplier to deliver social value in the delivery of this contract. Although the whole of the specification of this project could be considered as contributing to social value, this element is specifically focussed on how the evaluation contract is delivered by the Supplier and is not about the technical delivery methodology per se. Commitments on the inclusivity and benefits of the methodology should be included in the wider technical proposal.

Social value is not a specific costed activity but is an added co-benefit of delivery and an approach to delivery that is expected of all DSIT Suppliers.

10. Sub-contractors

The Supplier must have measures in place to manage any sub-contractors and ensure that their selection is conducted in an open and transparent manner.

11. Budget

The Buyer has maximum budget for this contract. The budget is up to £350,000 exclusive of VAT and non-UK taxes. Payment will be based on a Time and Materials basis unless agreed in writing by both parties for specific deliverables/milestones. This budget is for information only, there is no guaranteed volume of work and as such there is no obligation for the Buyer to spend any or all of this amount.

12. Payment

Tenderers will provide an invoice schedule as part of their Commercial Proposal which should take into consideration the estimated budgets and timelines. The Buyer would anticipate two invoices during the project delivery, but alternatives may be proposed by the Supplier.

Price will be fixed based on the commercial offers made. Payments, in GBP, will be linked to delivery of deliverables. The indicative milestones and phasing of payments is to be as detailed in the Pricing Annex.

Any payment conditions applicable to the prime Supplier must also be replicated with sub-contractors.

The Buyer aims to pay all correctly submitted invoices as soon as possible with a target of 10 days from the date of receipt of a compliant invoice and within 30 days at the latest in line with standard terms and conditions of Contract. We expect that this will be replicated in any sub-contractor arrangements and the Buyer may request evidence that this is the case.

The Buyer reserves the right to amend the Contract to increase the scope of activities required of the Supplier, so long as any additional activities meet the objectives of the Contract. Contract amendments would be managed by a formal variation process and will be made with mutual agreement with the Supplier. This is only permitted if the proposals are compliant within the remit of Public Contracts Regulations 2015.

13. Performance

The Buyer will manage the Contract and have regular performance discussions with the Supplier, at least every two weeks. Where the quality of deliverables are failing to meet the Buyer’s expectations identified in both these requirements and the Tenderer’s tender submission, the Buyer will work with the Supplier to identify measures to remedy these performance issues.

Where deliverables are taking significant rounds of comment from the Buyer prior to signing off as complete, the Buyer will only pay the amount given in the Contract and will not pay for additional drafting above and beyond expected. As such engagement with the Buyer during the drafting process to ensure that the final documents will be acceptable is essential.

The Supplier will be required to undertake appropriate, independent quality assurance of all deliverables and guarantee the accuracy of all outputs to DSIT. This could for example be carried out by an external academic.
The Supplier will be required to provide details of the quality assurance procedures they have in place in their bid. During the project, it will also be required to detail what quality assurance processes they have undertaken during the research.
The project should act in line with the research principles generally employed by HMG. The Service Provider will be required to provide the Customer access to all data used to produce the outputs for the Customer to carry out their own quality assurance processes.
AISI will expect the Supplier to:

- Respond to AISI queries within 2 working day
- Deliver high quality work in line with AISI guidance
- Apply problem solving and innovative thinking as appropriate to a nascent field of research
- Iterate outputs based on detailed feedback from AISI researchers
- Deliver work to tight timelines, which cannot be set at the outset of the project

Reference service levels here

14. Project Management

The Supplier is required to appoint a lead Project Manager, responsible for the Supplier's delivery of the contract. The Project Manager must have sufficient experience, seniority and time allocated to manage the project effectively. There will be one project lead from DSIT to liaise closely with the Supplier's Project Manager.
It is expected that following the project initiation meeting, regular contact will take place between the Supplier and DSIT by video-conference, telephone, email and face to face meetings. The frequency of contact will be agreed at the project inception meeting, however weekly project update meetings are required especially during the initial stages of the project and then a minimum requirement of every 2 weeks.
The Supplier is required on a weekly basis to provide a written update to DSIT on the research's progress, flag any emerging issues and risks and updates regarding the research itself and quality assurance (as and when applicable).
The Supplier is also required to provide feedback of emerging findings and key lessons during the course of the research at the weekly project meetings/calls. The format of how this will be presented will be agreed upon contract commencement.
If a consortium bid is submitted, the Supplier is required to explain any relevant lines of responsibility among consortium members, and proposed arrangements for management and liaison with the DSIT project manager.

15. Data Security

The Supplier is required to implement appropriate arrangements for data security at all times. Such procedures must meet the standards outlined in the framework terms and conditions, General Data Protection Regulation and the Data Protection Act.
Processes should be in place for data being returned by interviewers and safeguard against data loss, including appropriate risk management procedures.
The Supplier should confirm that such procedures will be implemented and outline the technical measures to be put in place to meet such requirements.

16. Ethical Conduct

The Supplier must have a clear approach for ensuring that the work is compliant with relevant ethical codes of conduct, as the Supplier is responsible for the ethical conduct of the research. The Supplier is required to set out any potential ethical issues presented by the research along with details of the arrangements for ethical scrutiny to ensure the day-to-day management of these risks. The Supplier will need to clearly explain how the information they provide will be stored, reported and protected and inform DSIT if this changes.
The Supplier must obtain consent from participants that makes it clear to participants that their data will be shared and used for research purposes.
The commissioning and management of the research should be carried out in accordance with Government Social Research ethics guidance[2] and the Data Protection Act 2018.

Annex 1 - DESNZ & DSIT Environmental Policy

DESNZ & DSIT Environmental Policy