|  |
| --- |
|  |
| **Statement of Requirement (SOR)** |
| **Contact & Project Information:** |
| **Project Manager** | Name | Redacted under FOI exemption Personal Information |
| Email | Redacted under FOI exemption Personal Information |
| Telephone number | Redacted under FOI exemption Personal Information |
| **Technical Partner** | Name | Redacted under FOI exemption Personal Information |
| Email | Redacted under FOI exemption Personal Information |
| Telephone number | Redacted under FOI exemption Personal Information |
| **iCas project number** | 711072 HWP030A |
| **Owning division** | CIS | Delivering division | CIS |
| Programme | AI Programme |
| Indicative task budget(s) £k | Core / initial work: | £100,000 - £120,000 | Options / follow on work: | £ |
|  |
| Innovation risk appetite: | Middle - Market development |
| Narrative (if applicable): |  |
| Using the Ansoff matrix below, please indicate your risk appetite with regards to accepting innovative bids/solutions. The type of analysis/experimentation technique is included within ‘Technology/Product’. |
|  |
| Use of Outputs: *(This section is used to inform risks, liabilities, mitigations and exploitation)* |
| Intended uses (including the approximate time before use and any key decisions that will use the output): |
| To inform the next phase of the study by identifying areas for further research or where useful products can be made relating to best practice. To inform the AI and AS experimentation hub of practices in use to inform their choices in adopting practices in the future.To inform conversations with the MOD on the future data needs and policies. Share with future suppliers under contract to inform future work. Publish work on a public forum (for example gov.uk or a blog) to highlight the work completed. |
| Possible uses: |
|  |
| Excluded uses: |
|  |
| Risk Assessment Process: Project teams are required to complete the ASTRID Liabilities spreadsheet that will look at the direct and indirect risks associated with the work. The assessment must be completed at the outset before the draft SOR is submitted, this will prevent delays and lessen negotiations when the proposal is received. The risk assessment spreadsheet can be found in the document list on the ASTRID Nexus Homepage: <http://org/org/ent/CME/ASTRID/SitePages/Home.aspx> Some generic risks are pre-filled so please ensure they apply to your task and delete/add as necessary. Each risk must be assessed in turn and a score entered in the spreadsheet. They will be automatically marked and a colour code produced. Please enter the results in the boxes below. A completed copy of the spreadsheet must be attached to this SOR when submitting it to the ASTRID Dstl PM for review and approval to release to CORDA.  |
| Direct Risk | **Green**  |
| In the event that a direct risk is scored as “Green” or “Yellow” the risk will be capped at pre-agreed limits of liability and the project team may continue with the submission of their requirement to CORDA once all necessary approvals have been issued by the Dstl ASTRID PM.In the event that a direct risk is identified as “Amber” or “Red” project teams should discuss the requirement with their Commercial POC before the task is submitted.  |
| Indirect/Consequential Risk | **Excluded**  |
| In the event that the indirect risk is “Excluded” project teams may continue with the submission of their requirement to CORDA once all necessary approvals have been issued by the Dstl ASTRID PM.In the event that the indirect risk is identified as “Included” project teams should discuss their requirement with their Commercial POC before the task is submitted. |
|  |
| Levels of Technical Assurance:The framework can offer three levels of Technical Assurance Support, and you have the ability to determine which level is suitable for your task. Full guidance listing the types of support under each level (and the trade-offs) can be found in the “ASTRID Guide – Levels of Assurer Support” [here](file:///%5C%5CRnet%5Corg%5CDIV_EXP%5CStandard%5C205_1_Reporting%5CFY2122%5CASTRID%5CASTRID_USER_DOCUMENTS%5CGUIDES%5CASTRID_GUIDE_LEVELS_OF_ASSURER_SUPPORT_V1.pdf) or in the document list on the [ASTRID Homepage](http://org/org/ent/CME/ASTRID/SitePages/Home.aspx). It may be that the level of support you require changes in the early discussion phase. Please ensure the final version of your SOR has the correct level indicated. Please indicate below which level you require  |
| Minimum [ ]  | Standard [x]  | Enhanced [ ]  |

Statement of Requirement (SoR)

|  |  |
| --- | --- |
| **Project’s document ref** | AST/AI & AS Data Best Practice Review SOR |
| **Version number** | **V1.0** |
| **Date** | **09/11/2021** |

|  |  |
| --- | --- |
| **1.** | **Requirement** |
| **1.1** | **Title (including AST/ prefix)** |
|  | AST086/AI & AS Data Best Practice Review |
| **1.2** | **Summary** |
|  | A key enabler to the Defence Artificial Intelligence (AI) and Autonomous Systems (AS) Experimentation Hub is data. As such we want to make sure the hub is using the most appropriate process, practices and policies to maximise exploitation of datasets for AI and Machine Learning applications, including increasingly Autonomous Systems. These datasets could be our own, owned by wider MOD and its suppliers or open source both newly created and already in existence. The Experimentation hub therefore wants to understand what process, practices and policies are currently in use or in research that are either seen as industry standard or are most effective for this purpose, by performing a literature review of open source information, summarising the findings and identifying any gaps in knowledge. |
| **1.3** | **Background** |
|  | Defence has established an AI and Autonomous Systems Experimentation Hub to catalyse the integration and adoption of these critical and ubiquitous capabilities at near-development speed for enduring technological superiority. The Experimentation Hub will conduct rapid AI and AS concept development and experimentation. To ensure maximum value can be extracted from the Experimentation Hub it requires good quality data, readily accessible, documented and in a format ready to use; and therefore needs the policies, process and practice to ensure the data it holds can be exploited in this way. For wider background and context see the newly published defence data strategy:<https://www.gov.uk/government/publications/data-strategy-for-defence>  |

|  |  |
| --- | --- |
| **1.4** | **Requirement** |
|  | Through a literature review of open source (1) industry, academia, government, NATO and partner nation information the task should identify and understand current and future potential good/best practice in data policy, process and practice for AI and Machine Learning use where this is either an industry standard or seen as the most effective way of doing things. The review should not focus on defence and its data problems, instead taking a broad, outward facing look at process and practice across all areas. Recommendations should not be defence specific, but pros and cons may take high level defence context (e.g. the newly published data strategy for defence) into account.The literature review must include some of the following areas in the context of AI and ML, with the final number and areas to be agreed with the supplier based on time and budget:* Synthetic Data – ensuring it is appropriate for use
* Data documentation, labelling, metadata and cataloguing – maximising discoverability, reuse and reducing duplication
* Data Standards and formats – promoting coherence to maximise reuse and interoperability
* Data architecture – promoting common enterprise wide solutions whilst allowing flexibility across the changing data landscape
* Data Assurance – ensuring data is correct, consistent, trusted and appropriate for use
* Data Creation –collecting and creating data in a way that makes it as useable as possible
* Data Wrangling – processes and policies to combine and refine datasets for best use

The investigation into each area should focus on practices for use with AI, ML and AS data, highlighting where this would differ from practices with datasets for other uses. It should consider the data as a whole but highlight where different types of data may have different practices. Data types include but isn’t limited to:* Tabular
* Video
* Imagery
* Voice
* Text
* Streaming
* Bulk

For each of these areas the work will produce written evidence including:* A summary of good/best practice in the area
* The pros and cons of the practice with respect to data for AI and ML use
* Enablers and barriers to putting the practice in place
* The readiness level of the practice (e.g. widely used, newly released etc.) and if in use which organisations are using the practice (e.g. US government, major industry players, UK MoD etc.)
* How this practice might develop with anticipated changes in AI/ML over the next 5-10 year timeframe (e.g. become obsolete)
* Any observed gaps in good/best practice across the areas
* Recommendations and the reasoning of what to adopt from each area, as well as any areas where further work would be beneficial (for example initiating research)
* An overall visual summary of the findings
1. If beneficial documents are identified by Dstl within the course of the contract and not available as open source, for example documents from government departments, they will be provided as GFA and recorded as such at the time.

**Contract Management**A kick off meeting with both supplier and Dstl teams should be held within 2 weeks of the contract starting to introduce the teams, the supplier to present and discuss the project plan and schedule and also discuss any risks to the project. The areas to cover as part of the literature review will also be agreed here. Monthly progress meetings should also be held to discuss:* Technical Progress
* Progress against schedule
* Commercial Aspects
* Risks and Issues
* Spend and forecast

If possible these meeting should be held virtually, to be decided between Dstl and the supplier at the time. Draft versions of the deliverables should be provided to Dstl no less than 20 working days before the final deliverable date **Timelines for delivery**The work should be completed and delivered to Dstl by 29th April 2022  |
| **1.5** | **Options or follow on work**  |
|  | Depending on outcome of the work we may require additional areas added for investigation, for example Data Sharing or APIs, at a later date.We may also require the supplier to publish the findings further in the public domain, for example a blog post or to a journal, subject to future contractual agreements. We may also choose to investigate more deeply into some identified areas and create further products, such as best practice guides, subject to future contractual agreements. **An indicative Rough Order of Magnitude (ROM) cost is required for the options above.** |

|  |  |
| --- | --- |
| **1.6** | **Deliverables & Intellectual Property Rights (IPR)** |
| **Ref.** | **Title** | **Due by** | **Format** | **TRL\*** | **Expected classification (subject to change)** | **What information is required in the deliverable** | **IPR DEFCON/ Condition***(Commercial to enter later)* |
| *D1* | *Final Report and presentation* | *By 29th April 2022* | *Word document (.docx) to be a maximum of 50 pages and a Summary presentation (.pptx)* | *n/a* | *O* | *Report Deliverable to include but not limited to:* * Information as detailed in the requirements
* Approach taken
* List of relevant sources reviewed
* Visual representation of findings

*Presentation deliverable to include but not limited to:* * A summary of the information as detailed in the requirements and final report deliverable
 | DEFCON 703 |

\***Technology Readiness Level required, if applicable**

|  |  |
| --- | --- |
| **1.7** | **Standard Deliverable Acceptance Criteria** |
|  | **Deliverable Acceptance Criteria (**As per ASTRID Framework T&Cs)1. Acceptance of Contract Deliverables produced under the Framework Agreement shall be by the owning Dstl or wider Government Project Manager, who shall have up to 30 calendar days to review and provide comments to the supplier.
2. Task report Deliverables shall be accepted according to the following criteria except where alternative acceptance criteria are agreed and articulated in specific Task Statements of Work:
* All Reports included as Deliverables under the Contract e.g. Progress and/or Final Reports etc. must comply with the Defence Research Reports Specification (DRRS) which defines the requirements for the presentation, format and production of scientific and technical reports prepared for MoD. Reports shall be free from spelling and grammatical errors and shall be set out in accordance with the accepted Statement of Work for the Task.
* Interim or Progress Reports: The report should detail, document, and summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; substantive performance; a description of current substantive performance and any problems encountered and/or which may exist along with proposed corrective action. An explanation of any difference between planned progress and actual progress, why the differences have occurred, and if behind planned progress what corrective steps are planned.
* Final Reports: shall describe the entire work performed under the Contract in sufficient detail to explain comprehensively the work undertaken and results achieved including all relevant technical details of any hardware, software, process or system developed there under. The technical detail shall be sufficient to permit independent reproduction of any such process or system.
1. Failure to comply with the above may result in the Authority rejecting the Deliverables and requesting re-work before final acceptance.
2. Acceptance criteria for non-report Deliverables shall be agreed for each Task and articulated in the Statement of Work provided by the Contractor
 |
| **1.8** | **Specific Deliverable Acceptance Criteria** |
|  | The deliverables must meet the criteria specified in the sections above.All deliverables shall be Microsoft Office compatible format and delivered via email to the Dstl Technical Partner.* Draft versions of final deliverables will be provided to Dstl by the supplier no less than 20 working days prior to the final deliverable date.

The criteria for accepting deliverables is as follows:* Documents are sufficiently detailed and technically coherent to enable a member of Dstl’s technical team to understand the scientific progress made and that the content meets the needs of the requirement.
* Final deliverables (word document and summary PowerPoint) should be written in a way that is understandable for non-technical audiences with little knowledge of AI, ML, AS or Defence.
 |

|  |  |
| --- | --- |
| **2.** | **Quality Control and Assurance** |
| **2.1**  | **Quality Control and Quality Assurance processes and standards that must be met by the contractor** |
|  | [ ]  **ISO9001**  (Quality Management Systems)[ ]  **ISO14001** (Environment Management Systems)[ ]  **ISO12207** (Systems and software engineering — software life cycle)[ ]  **TickITPlus**  (Integrated approach to software and IT development)[ ]  **Other:**  (Please specify)  |
| **2.2**  | **Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement** |
|  | n/a |

|  |  |
| --- | --- |
| **3.** | **Security** |
| **3.1** | **Highest security classification** |
|  | **Of the work** | O |
| **Of the Deliverables/ Output** | O |
| Where the work requires more than occasional access to Dstl premises (e.g. for meetings), SC Clearance will be required. |
| **3.2** | **Security Aspects Letter (SAL) – Note the ASTRID framework has an overarching SAL for quotation stage (up to OS)** |
|  | Not applicableIf yes, please see SAL reference- *Enter iCAS requisition number once obtained* |
| **3.3** | **Cyber Risk Level** |
|  | Very low |
| **3.4** | **Cyber Risk Assessment (RA) Reference**  |
|  | RAR-297993248This must be completed before a contract can be awarded. In accordance with the [Supplier Cyber Protection Risk Assessment (RA) Workflow](https://www.gov.uk/government/publications/supplier-cyber-protection-service-risk-assessment-workflow) please complete the Cyber Risk Assessment available at <https://suppliercyberprotection.service.xgov.uk/>  |

| **4.** | **Government Furnished Assets (GFA)** |
| --- | --- |
| GFA to be Issued - No*If ‘yes’ – add details below. If ‘supplier to specify’ or ‘no,’ delete all cells below.*  |
| **GFA No.** | **Unique Identifier/ Serial No** | **Description:***Classification, type of GFA (GFE for equipment for example), previous MOD Contracts and link to deliverables* | **Available Date** | **Issued by** | **Return or Disposal** *Please specify which* |
|  |  |  |  |  |  |
| **If GFA is to be returned:** It must be removed from supplier systems and returned to the Dstl Project Manager within 2 weeks of the final Task deliverable being accepted. (Any required encryption or measures can be found in the Security Aspects Letter associated with the Task).**If GFA is to be destroyed:** It must be removed from supplier systems and destroyed. An email confirming destruction should be sent to the Dstl Project manager within 2 weeks of the final Task deliverable being accepted |

| **5.**  | **Proposal Evaluation** |
| --- | --- |
| **5.1** | **Technical Evaluation Criteria** |
|  | Process will be as per ASTRID Framework T&Cs. If particular attention should be paid to certain aspects of the requirement, please confirm here:Capability statements must include recent examples of work completed relating to AI and also horizon scanning to demonstrate proficiency in these areas. |
| **5.2** | **Commercial Evaluation Criteria**  |
|  | As per ASTRID Framework T&Cs.  |