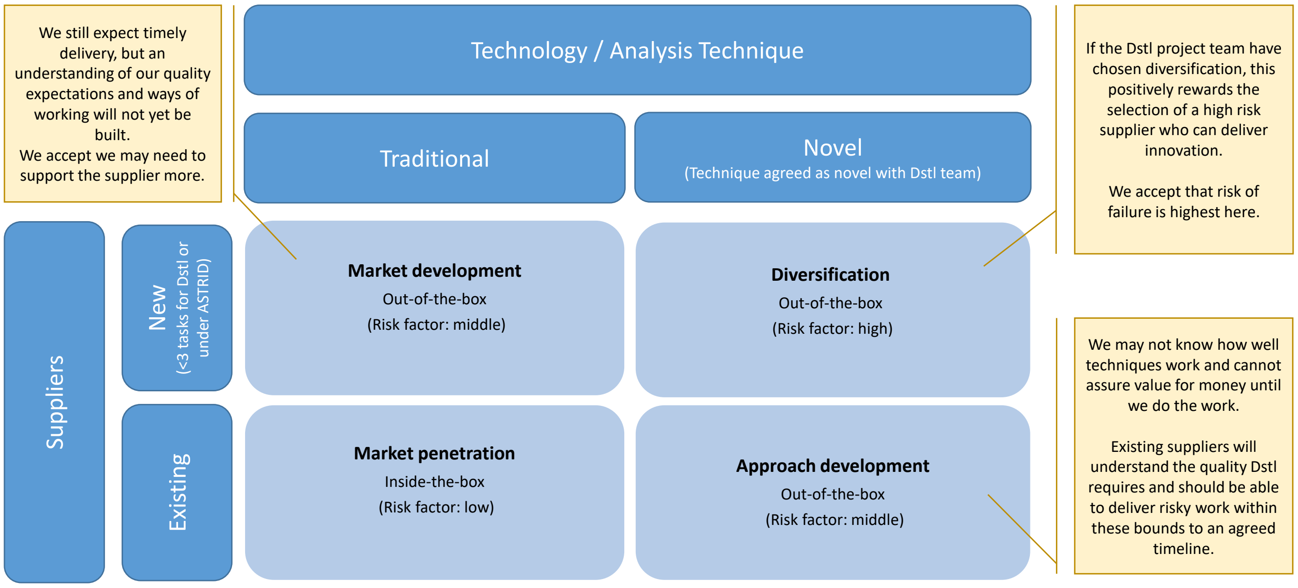
ASTRID
ANALYSIS FOR SCIENCE & TECHNOLOGY RESEARCH IN DEFENCE

Statement of Requirement (SOR)

Contact & Project Information:

Project Manager	Name	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
	Email	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
	Telephone number	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
Technical Partner	Name	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
	Email	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
	Telephone number	[REDACTED UNDER FOI SECTION 40 - PERSONAL INFORMATION]		
iCas project number	[REDACTED UNDER FOIA SECTION 26 – DEFENCE]			
Owning division	Exploration	**Delivering division**	Exploration	
Programme	Defence Science & Technology Futures			
Indicative task budget(s) £k	Core / initial work:	£ 400k	Options / follow on work:	£150k

Innovation risk appetite:	High
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'.	



We still expect timely delivery, but an understanding of our quality expectations and ways of working will not yet be built.
We accept we may need to support the supplier more.

		Technology / Analysis Technique	
		Traditional	Novel (Technique agreed as novel with Dstl team)
Suppliers	New (<3 tasks for Dstl or under ASTRID)	**Market development** Out-of-the-box (Risk factor: middle)	**Diversification** Out-of-the-box (Risk factor: high)
	Existing	**Market penetration** Inside-the-box (Risk factor: low)	**Approach development** Out-of-the-box (Risk factor: middle)

If the Dstl project team have chosen diversification, this positively rewards the selection of a high risk supplier who can deliver innovation.

We accept that risk of failure is highest here.

We may not know how well techniques work and cannot assure value for money until we do the work.

Existing suppliers will understand the quality Dstl requires and should be able to deliver risky work within these bounds to an agreed timeline.

Use of Outputs:
This section is used to inform risks, liabilities, mitigations and exploitation. Questions 1-10 below should be a Yes/No/NA response. Please indicate if the questions do not make sense in the context of your task.
Intended uses (including the approximate time before use and any key decisions that will use the output):
The DTM application will be actively used on Dstl and MOD networks.
Possible uses:
Outputs shared across UK Government departments as well as International Partners.
Excluded uses:

1	Will any output be directly used as part of a safety critical system, or will it be one of the most important factors in decisions on Cat A/B investments (>£100M), or at Ministerial level policy making?	N
2	Is this task collating and presenting previous work without making further / new recommendations?	N
3	Is this task research - for example, an exploration of new methods, models or tools?	N
4	Will a re-run of the modelling or analysis be required before outputs are presented to a decision maker?	NA
5	Will the outputs form a minor part of the work that will be combined by the Dstl Project Team before being used for decision-making?	Y
6	Has the approach to the work (how to undertake the work) been fixed by Dstl/MOD?	N
7	Will 100% of the technical assurance of the outputs provided by the Dstl Project Team?	N
8	Is the Dstl Project Team capping the maximum levels of verification and validation to be carried out on outputs?	N/A
9	Is this task developing or maintaining a method, model or tool (MMT) which will be used for multiple use cases over a period of time by Dstl Project Teams?	Y
10	Can you confirm that there are no known intended uses of the outputs over and above those described here that could result in new risks if the output was incorrect?	N/A

Statement of Requirement (SoR)

Project's document ref	**ASTRID077-SOR-DTM-O**
Version number	**1.0**
Date	**21/09/2021**

1.	**Requirement**
1.1	**Title (including AST/ prefix)**
	AST077/Defence Technology Matrix (DTM) software support
1.2	**Summary**
	Defence Technology Matrix (DTM) is an intelligent platform that allows users to *view, collate, refine* and *discuss* defence-relevant S&T to explore how *'technologies'* might *work together* to deliver military effects. It is underpinned by a *managed* repository of new and emerging technology *summary information*. And supports *current* challenges through to *future concepts*, helping Defence to be more agile in aligning short-term planning with longer-term foresight. This SOR is for software support for the DTM application in line with Defence Digital guidance.
1.3	**Background**

	Extracted from Contracting for Software Support document from 2016[1]. Software support can be broken down into two distinct yet interrelated components – Software Operations Support (SOS) and Software Modification. Software Operations Support (SOS) • SOS includes all the activities that occur on a day-by-day basis relating to the preparation, and where necessary recovery, of software dependent systems. • Good SOS enables the effective operational use of a system and contributes directly to system availability. Software Modification • Software modification includes all the activities that enable software to be changed in a controlled and timely manner to meet new or altered requirements. • Software modification relates to our ability to exploit software as the means by which we will keep our systems current, sustaining capability in an ever changing threat environment. • Good software modification enables capability sustainment and contributes to system availability. Differences between SOS and Software Modification The main distinction between the two support functions is: • SOS is an operational support function carried out at the same tempo as the equipment being used. • Software Modification is carried out ‘off-line’ away from where the equipment is used.

[1] http://aof.uwh.diif.r.mil.uk/aofcontent/tactical/software/downloads/20160613-Contracting_For_Sw_Support-U.doc

1.4	Requirement

From the perspective of what support we would require from a contractor these are:

1. Security updates as well as those directed by MODCERTs. This is part of SOS.
2. Software update to cover fixes and minor updates. This can include changes due to hosting environments. Could include provision of user support (such as Helpdesk User support). This includes both SOS and Software Modification.
3. Software functionality features as per user requests. This is Software Modification.

Dstl needs to ensure that at least the first two support elements are covered in order to maintain agreement with any JSP604 approval. In addition the supplier is to provide a method to capture the technical debt, the impact on DTM and the associated costs to address them. This will be shared with Dstl so that project risks are fully understood.

User Acceptance Test (UAT) will be required at a minimum for software modification support (functionality features).

Supplier is able to suggest different models that address the requirements above. Some suggestions are:

- Structured Sprints
  - Up to 3 Sprints per year to cover software updates (including those directed by MODCERTS).
  - Up to 4 sprints per year to provide functionality features.
  - Sprints to be enacted as and when. To start within 4-8 weeks of formal request. Interested in trade-offs.
  - Sprints are estimated to be two weeks in time with the required resource to deliver the requirements.
- Support expressed in days.
  - Support could be expressed in days which allow for varied levels of support during the year. This could be delivered in different ways such as sprints or ad-hoc days.
  - An **example** could be 3 people for 10 days on the sprints (assuming two weeks) with additional days for ad-hoc support. This example would give a total of 230 days (up to 7 sprints of 30 man days with 20 days for ad-hoc support) over a year.

With the rollout of DTM onto MODNET in late FY21/22 there is likely to be surge requirements to ensure that the rollout is fully supported.

Procurement approach

Under JSP604 Rule 16 (ICT capabilities and services shall be designed to provide a high-quality product, meeting the customers’ requirements for reliability, maintainability, usability and

	serviceability thereby permitting holistic service management) and JSP604 Rule 17 (ICT shall have defined support arrangements) we need to ensure that there is a suitable support wrap for DTM and that it is funded through life. Provide there remains a need for DTM (under current DSTF programme this is for the next two years) we will be moving DTM to be more of a service. Details on Service Management are within JSP604.
1.5	**Options or follow on work**
	As part of the long term support to DTM as a service a longer term support contract will be needed. The design of this will be dependent on how Defence intends DTM to be funded long term. This would need to be contracted before the end of this SOR. The performance of this ASTRID SOR will inform the longer term support contract. Options required for additional structured sprints or support days.

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)*
D - 1	Updated DTM application and code	End of Sprints	Java war file, updated GitHub and associated documentation	n/a	[REDACTED UNDER FOIA SECTION 24 – NATIONAL SECURITY]	At a minimum: • DTM application war file • Code updated on DTM repository (currently GitHub) • Updated test results and documentation • Updated documentation such as User Guide • Updated Knowledge Asset (KA) for MODNET SPOC as required.	

*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.

3. Failure to comply with the above may result in the Authority rejecting the Deliverables and requesting re-work before final acceptance.

4. 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

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**

3.	**Security**	
3.1	**Highest security classification**	
	Of the work	[REDACTED UNDER FOIA SECTION 24 – NATIONAL SECURITY]
	Of the Deliverables/ Output	[REDACTED UNDER FOIA SECTION 24 – NATIONAL SECURITY]
	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 applicable If yes, please see SAL reference- *Enter iCAS requisition number once obtained*	
3.3	**Cyber Risk Level**	
	[REDACTED UNDER FOIA SECTION 26 – DEFENCE]	
3.4	**Cyber Risk Assessment (RA) Reference**	
	[REDACTED UNDER FOIA SECTION 26 – DEFENCE] If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available at https://supplier-cyber-protection.service.gov.uk/	

4. Government Furnished Assets (GFA)

GFA to be Issued - Yes

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*
GFA-1		DTM code via Dstl owned private GitHub repository			Disposal of any copies

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**
5.2	**Commercial Evaluation Criteria**
	As per ASTRID Framework T&Cs.