

Statement of Requirement (SOR)

Contact & Project Information:

Redacted under FOIA Section 40 - Personal Information

Project Manager	Name			
	Email			
	Telephone number			
Technical Partner	Name			
	Email			
	Telephone number			
CHESS PJ Number	PJ100686	CHESS Leaf Code	EMR	
Owning division	EXP	Delivering division	EXP	
Programme	Defence Science & Technology Futures (DSTF)			
Indicative task budget(s) £k	Core / initial work:	£120k	Options / follow on work:	£0

Innovation risk appetite:	Middle - Approach development
Narrative (if applicable):	Although we are initially seeking approaches known to work, we are willing to experiment with novel approaches if additional benefits may be realised.

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'.

		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)	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.
	Existing	Market penetration Inside-the-box (Risk factor: low)	Approach development Out-of-the-box (Risk factor: middle)	
				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)***Intended uses** (including the approximate time before use and any key decisions that will use the output):

The approach will be demonstrated when new defence concepts are proposed. After review, the concepts may be developed further. If successful, the approach will be re-used to generate further defence concepts. The decision to progress a concept will be taken within 2 months of its generation. The outputs will not be used to inform any key decisions.

The approach will be shared with MOD and may also be shared with industry as part of any further concept development work.

Possible uses:

An approach that combines individual technical ideas into a larger technical idea might be used in any situations where component ideas are to be combined into a larger idea e.g. combining policy options into an overall policy.

Excluded uses:

The proposed approach will not provide the only source of defence concepts.

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](#)

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 [Dstl ASTRID PM](#) for review and approval to release to CORDA.

Direct Risk

Yellow

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](#) or in the document list on the [ASTRID Homepage](#).

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 <input type="checkbox"/>	Standard <input checked="" type="checkbox"/>	Enhanced <input type="checkbox"/>
----------------------------------	--	-----------------------------------

Statement of Requirement (SoR)

Project's document ref	Task 186
Version number	V1.1
Date	26/09/2022

1.	Requirement
1.1	Title (including AST/ prefix)
	AST186/Creating Concepts
1.2	Summary
	<p>The Identify project within the DSTF programme seeks to generate new 'game changing' Futures defence concepts that can subsequently be developed, refined and exploited. 'Concepts' are defined here as outline descriptions of ideas and combinations of technologies that could provide benefits to Defence.</p> <p>An approach is needed to consistently generate new concepts. The approach should be:</p> <ul style="list-style-type: none">• Based on known successful formats and techniques• Evolved collaboratively to develop and share expertise• Piloted using 'live' information• Adapted and improved as required• Capable of being used repeatedly to generate further concepts <p>The approach should be shown to generate concepts by December 2022, in order to meet a DSTF programme-critical deadline. The approach should then be used to generate further concepts by February 2023, and the findings reported by March 2023.</p>
1.3	Background

The Identify project seeks to propose 'game changing' concepts. These are not intended to solve today's problems, but will transform Defence beyond the generation after next. Ideas and 'weak signals' need to be interpreted and combined into embryonic defence concepts that can be developed further.

'Create' sessions have been held to date, at which Dstl staff with different technical expertise came together to propose alternative applications of different ideas. These sessions usually developed individual ideas, which are inherently small in scope. Game changing concepts are more likely to be combinations of individual ideas.

Alternative approaches to concept generation are sought that can combine ideas, contexts and needs into concepts of potentially game changing impact and benefit.

1.4	Requirement
	<p>Taking a systems view, the supplier is requested to propose an approach or framework to consistently enable the generation of new concepts. The approach should recommend:</p> <ul style="list-style-type: none"> • Information and expertise needed to generate new concepts • Who should be involved in concept generation and their roles and responsibilities • Tools and methods to support the synthesis of emerging technologies into viable new concepts • Types of evidence likely to be needed to enable a new concept to be handed over for subsequent exploitation <p>This should be completed in three phases:</p> <p>Phase 1: Propose an approach to generating new concepts, through collaboration and joint development</p> <p>Phase 2: Hold workshop(s) with Dstl analysts (list to be provided by the Dstl Technical Partner) to pilot approach using 'live' information, review output and findings, and adapt approach as required</p> <p>Phase 3: Use the updated approach to propose three new defence concepts using 'live' information, and involve Dstl analysts (list to be provided by the Dstl Technical Partner). Hold a workshop to review the outputs and approach.</p> <p>The approach should be evolved collaboratively between the supplier and Dstl to develop and share knowledge and expertise.</p>
1.5	Options or follow on work
	Not Applicable

1.6 Deliverables & Intellectual Property Rights (IPR)							
Ref.	Title	Due by (MUST Use T0+)	Format	TRL*	Expected classification (subject to change)	What information is required in the deliverable	IPR DEFCON/ Condition (Commercial to enter later)
D - 1	Proposed Approach	T0+1 (Nov 22)	Any	n/a	Redacted under FOIA Section 26 - Defence	Written description of proposed approach and format of outputs that would allow others to adopt the approach. An engaging format should be used, not necessarily a 'report'	
D - 2	Workshop Output	T0+2 (Dec 22)	Any	n/a		<p>Written descriptions of:</p> <ul style="list-style-type: none"> Initial proposed defence concept In light of experience, summary and reasoning behind any proposed changes to approach and defence concept format Updated approach and defence concept format <p>The description of the updated approach should allow others to apply the approach. An</p>	

						engaging format should be used, not necessarily a 'report'. The initial defence concept should be written in a format to be agreed	
D - 3	Final Report	T0+4 (Feb 23)	Any	n/a	Redacted under FOIA Section 26 - Defence	Written descriptions of three proposed defence concepts, in a format to be agreed	

*Technology Readiness Level required, if applicable

1.7	Standard Deliverable Acceptance Criteria
	<p>Deliverable Acceptance Criteria (As per ASTRID Framework T&Cs)</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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
	<p>The supplier should define and agree the minimum standard required for a new concept, and demonstrate the deliverables meet that standard.</p>

2.	Quality Control and Assurance
2.1	Quality Control and Quality Assurance processes and standards that must be met by the contractor
	<input type="checkbox"/> ISO9001 (Quality Management Systems) <input type="checkbox"/> ISO14001 (Environment Management Systems) <input type="checkbox"/> ISO12207 (Systems and software engineering — software life cycle) <input type="checkbox"/> TickITPlus (Integrated approach to software and IT development) <input type="checkbox"/> Other: (Please specify)
2.2	Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement
	None

3.	Security	
3.1	Highest security classification	
	Redacted under FOIA Section 26 - Defence	
	Of the work	
	Of the Deliverables/ Output	
	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)	
	Redacted under FOIA Section 26 - Defence	
	If yes, please see SAL reference- <i>Enter iCAS requisition number once obtained</i>	
3.3	Cyber Risk Level	
	Redacted under FOIA Section 26 - Defence	
3.4	Cyber Risk Assessment (RA) Reference	
	Redacted under FOIA Section 26 - Defence	
	This must be completed 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://suppliercyberprotection.service.xgov.uk/	

4. Government Furnished Assets (GFA)

GFA to be Issued - Choose an item.

If 'yes' – add details below. If 'supplier to specify' or 'no,' delete all cells below.

GFA No.	Unique Identifier/ Serial No	Description: <i>Classification, type of GFA (GFE for equipment for example), previous MOD Contracts and link to deliverables</i>	Available Date	Issued by	Return or Disposal <i>Please specify which</i>
GFA-1		A list of example creativity techniques will be provided at the bidding stage – This is for awareness only and it is not required they should be used	With SOR	Redacted under FOIA Section 40 - Pers	Disposal

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