Serapis Tasking Form

Tasking Form Part 1: *(to be completed by the Authority's Project Manager)*

To:	Lot 6 Frazer-Nash Consultancy Ltd	**From:**	The Authority

Any Task placed as a result of your quotation will be subject to the Terms and Conditions of Framework Agreement Number:

LOT 6 DSTL/AGR/SERAPIS/UND/01

VERSION CONTROL

0.1

REQUIREMENT

Proposal Required by:	31/08/2021	**Task ID Number:**	U48
The Authority Project Manager:	[REDACTED UNDER FOIA EXEMPTION]	**The Authority Technical Point of Contact:**	[REDACTED UNDER FOIA EXEMPTION]
Task Title:	Open Call - Autonomous Decision Making for Cyber Defence		
Required Start Date:	30/09/2021	**Required End Date:**	31/03/2022
Requisition No:	[1000166607	**Budget Range**	£750k

TASK DESCRIPTION AND SPECIFICATION

Serapis Framework Lot	☐ Lot 1: Collect ☐ Lot 2: Space systems ☐ Lot 3: Decide ☐ Lot 4: Assured information infrastructure ☐ Lot 5: Synthetic environment and simulation ☒ Lot 6: Understand

Statement of Requirements (SOR)

Open Call - Autonomous Decision Making for Cyber Defence

Background

In response to operational demands, military networks and systems are becoming more complex and interconnected, both internally and with allies, and also with commercial and civilian infrastructure. Timely information sharing and cross-boundary information flows are critical to mission success. In parallel, attacks are becoming more sophisticated, with potentially greater impact on military operations. Identifying, selecting and carrying out cyber defence responses in a timely manner is essential.

The Autonomous Resilient Cyber Defence (ARCD) project is funded for 4 years and aims to research and develop self-defending, self-recovering concepts for military platforms and technologies. The goal is to deliver a new paradigm in Cyber Defence, reducing the time it takes to respond to incidents and ensuring freedom of action.

Key to realising this goal will be the development of autonomous agents that can respond to adversary activity on networks and systems without human intervention. These agents will need to operate with incomplete or

uncertain data, reason over a range of (potentially complex) response options, evaluate the risks and impact of selected approaches and continuously monitor for unintended consequences. These agents may need to operate in edge environments where compute capability is scarce, and should ideally provide explainable justification for their actions

Requirement

Under this open call, the Authority is seeking novel Artificial Intelligence (AI) and Machine Learning (ML) approaches for autonomous cyber defence decision making. Specifically, the Authority is interested in research that aims to:

- Develop AI and ML based approaches for autonomous response options planning. This could include (but is not limited to) the application of reinforcement learning, adversarial machine learning, game theory etc. Response options could include (but are not limited to): implementation of technical mitigation measures; initiating actions to increase information veracity or certainty before implementing a mitigation response; or initiating actions to identify the cause of system failure in order to recover from it.
- Develop multi agent approaches and architectures for cyber defence decision making. Key aspects include the trade-off between centralised and de-centralised agents, approaches for information sharing between agents, agent hierarchy and multi agent consensus. Note that this should focus on the interaction of machine agents and not the interaction of humans with machine agents.
- Develop methods and approaches to evaluating the decisions generated by the agents to determine their effectiveness and impact

The Authority is not seeking proposals that:

- provide solutions, or demonstrations of solutions, which are already commercial products (or are included as part of commercial products / cybersecurity platforms)
- focus on the detection of anomalous or malicious activity. This is covered by other elements of the Dstl and wider government research programmes and is not in scope for this IFA. This IFA is specifically focussed on approaches to determine and evaluate machine based decision making.
- aim to solely develop training environments for autonomous agents. This is covered by other elements of the Dstl and wider government research programmes and is not in scope for this IFA.
- aim to conduct literature reviews, technology watch, horizon scanning, roadmaps or technology prediction.
- offer demonstrations of off-the-shelf products requiring no experimental development (unless applied in a novel way to the challenge)
- offer no real long-term prospect of integration into defence and security capabilities
- offer no real prospect of out-competing existing technological solutions

Suppliers may propose more than one idea across these different resrach themes. However, each idea must be proposed separately. The proposal should provide a specific description of the technology concept and describe the work to be conducted.

Outcomes

It is anticipated that the specific outcomes of each funded project will be dependent on the nature of the proposed work and likely TRL of the solution. However, as a guide, the Authority is looking for:

- A report that summarises the key concepts and describes the function of the solution in detail. This is intended to be shared with MOD, wider UK government and potentially Five Eyes partners. Where there is background IP, suppliers should produce two reports – one with, and one without, background IP.
- A proof of concept implementation and associated source code and other software artifacts (such as training data etc.) Where there is background IP, the supplier should structure the implementation such that background IP can be separated from work funded by ARCD (e.g. background IP provided as separate softare executable code).
- A demonstration event to exhibit the capabilities of the proof of concept solution.

Project Management

The supplier shall arrange a kick-off meeting within 1 week of the projct start date. The outputs of this meeting will be captured in a set of minutes that will be delivered to the Authority.

Unless otherwise agreed with the Autohrity, the supplier shall produce bi-weekly progress reports covering the status of the work, risks, opportunities and issues related to delivery. These reports can be delivered via email.

The supplier shall identify and request any Government Furnished Assets (GFA) needed to complete the activity. Any GFA provided must be managed by the supplier in accordance with a Security Aspects Letter (SAL).

The supplier shall arrange a close down meeting to take place no later than 1 week prior to the end of the contract. This meeting shall serve as a contract closure meeting and as a forum in which to collate lessons identified.

Next Steps / Exploitation

Successful outputs may be taken forward under the ARCD project. Where compatible, the intent is to integrate technologies into an ARCD framework (currently under development), which will be used as the platform for technology demonstration at the end of the project. However, it is anticipated that some proposed solutions or technologies may be better suited for standalone operation. In some cases, it may also be possible to deploy capabilities onto operational cyber defence systems to support operator decision making.

Successful solutions may be shared with Five Eyes (Australia, Canada, UK, US and New Zealand) partners through a Technical Panel (TP) of The Technical Cooperation Program.

Budget

The Authority is seeking proposals for short (≤6 months) term research projects. Individual proposals are expected to be in the range £100-£150K (≤6 months). We estimate that 5-7 tasks will be funded. Proposals must complete in full by March 2022. It is expected that these studies to yield low Technical Readiness Level (TRL 2 to 4) output. We may wish to fund follow on work or further activity to mature technologies to higher TRLs in subsequent phases of the ARCD project if they are shown to have merit.

Proposals that are unsuccessful in this initial Open Call may be considered in subsequent years.

Procurement Strategy

☒ Lot Lead to recommend ☐Single Source / Direct Award

Pricing:

☒ Firm Pricing ☐ Ascertained Costs* ☐ Other*

Firm Pricing shall be in accordance with DEFCON 127 and DEFCON 643

Ascertained Costs shall be in accordance with DEFCON 653 or DEFCON 802.

*only at Authority's discretion

Task IP Conditions

Task IP Conditions (Follow the NIPPY guide to identify your information and IP requirements for each deliverable)	**Summary of the Authority's rights in foreground IP (IP generated by the supplier in performance of the contract)**
DEFCON 703 ☐	Vests ownership with the Authority
DEFCON 705 Full Rights ☒	Enables MOD to share in confidence as GFI or IRC under certain types of agreements. Can be shared in confidence within UK Government.
OTHER IP DEFCONS: 14* ☐, 15* ☐, 16* ☐, 90* ☐, 91* ☐, 126* ☐	Generally only suitable for deliverables at TRL 6 and above.

BESPOKE IP Clause ☐ *	Details to be added and agreed by IP Group
* Do not use without IPG advice and approval	
Please state in this text box if MOD or the customer has a requirement a) that one or more Other Government Departments is able to share confidentially with their own suppliers, b) to publish but you do not think there is a requirement to own or control the deliverable, or c) to share under a procurement Memorandum of Understanding (MOU).* *If any of these three issues applies, please contact IPG for advice before completing this form. *Listing research MOUs is not required, but can be a helpful courtesy to the supplier.*	

DELIVERABLES

Ref	Title	Due by	Format	Expected classification (subject to change)	Information required in deliverable	IPR DEFCON
D-1	Bi-weekly Progress Updates	T0+2 weeks (recurring every two weeks subsequently)	Presentation (.pptx or .pdf)	Official	Presentation pack to include but not limited to: • Update on technical progress • Progress report against project schedule. • Review of risks and issues • Commercial aspects. • Review of deliverables.	705
D2	Summary Report	31/03/2022	Technical Report (.docx, .odt or .pdf)	Official / Official-Sensitive	A report int ehs supplier's chosen template that summarises the key concepts and describes the function of the solution in detail. The report shall contain the DEFCON IP conditions and report documentation page. This may be shared with MOD, wider UK government and potentially Five Eyes partners. Where there is background IP, suppliers should produce two reports – one with, and one without, background IP.	705

D3	Software Source Code and Artefacts	31/03/2022	Git repository	Official / Official-Sensitive	Shall include all source code and artefcats (for example, training data) generated in support of the task.	705
D4	Software Executable Code	31/03/2022	Software executables	Official / Official-Sensitive	Where necessary, this shall include all executable code (or compiled byte code) and files required to run the software.	705
D5	Demonstration Event	2 weeks before contract end	Demonstration	Official / Official-Sensitive	End of project capability demonstration to the Authority and UK MoD and UK Government stakeholders identified by the Authority.	705

DELIVERABLE: ACCEPTANCE / REJECTION CRITERIA

Unless otherwise stated below, Standard Deliverable Acceptance / Rejection applies. This is 30 business days, in accordance with DEFCON 524 Rejection, and DEFCON 525 Acceptance.

Standard Deliverable Acceptance / Rejection:-

Yes ☒ (DEFCON 524 Rejection, and DEFCON 525 Acceptance)

No ☐ (if no, please state details of applicable criteria below)

Deliverable Acceptance / Rejection Criteria:-

If there are any other specific acceptance/rejection criteria you would like to apply to any of the deliverables, please state them here.

Government Furnished Assets (GFA)

ISSUE OF EQUIPMENT/RESOURCES/INFORMATION/FACILITIES (*if not applicable, delete table and insert "None" in this text box)*

None

QUALITY STANDARDS

☒ **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 in free text below)

SECURITY CLASSIFICATION OF THE WORK

The highest classification of this SOR

OFFICIAL ☒ OFFICIAL-SENSITIVE ☐ SECRET ☐ TOP SECRET ☐ STRAP ☐ SAP ☐

The highest expected classification of the work carried out by the contractor

OFFICIAL	☐	OFFICIAL-SENSITIVE	☒	SECRET	☐	TOP SECRET	☐	STRAP	☐	SAP	☐

The highest expected classification of Deliverables/Output

OFFICIAL	☐	OFFICIAL-SENSITIVE	☒	SECRET	☐	TOP SECRET	☐	STRAP	☐	SAP	☐

Is a Security Aspects Letter (SAL) required? *(A Security Aspects Letter (SAL) will be required for each Task above Official-Sensitive and above)*

Yes ☒ No ☐

TASK CYBER RISK ASSESSMENT. *(In accordance with DEF STAN 05-138 and the* Risk Assessment Workflow)

Cyber Risk Level	Very Low
Risk Assessment Reference	228738446

ADDITIONAL TERMS AND CONDITIONS APPLICABLE TO THIS CONTRACT

Not applicable

Please ensure all completed forms are copied to DSTLSERAPIS@dstl.gov.uk when sending to the Lot Lead.

Tasking Form Part 2: *(To be completed by the Lot Lead)*

To: The Authority	From: The Lot Lead

Proposal Reference 013235-95987L U48 Autonomous Decision Making for Cyber Defence - Frazer-Nash Proposal **(attached)**

Delivery of the requirement:

The proposal <u>shall</u> include, but not be limited to:

- A full technical proposal that meets the individual activities that are detailed in Statement of Requirements (Part 1 to Tasking Form).
- Breakdown of individual Deliverables, with corresponding Intellectual Property rights applied.
- Breakdown of Interim Milestone Payments, with corresponding due dates.
- A work breakdown structure/project plan with key dates and deliverables identified.
- A list of required Government Furnished Assets from the Authority, including required delivery dates.
- A clear identification of Dependencies, Assumptions, Risks and Exclusions which underpin your Technical Proposal.
- Sub-Contractors Personnel Particulars Research Worker Form and security clearances (if applicable)

PRICE BREAKDOWN

You are to use the costs detailed in Item 2 Table I in the Schedule of Requirement and at Annex E Table 2 of the Serapis Framework Agreement. Please also provide a price breakdown which should include, but is not limited to: Lot Lead Rates, Sub-contractors costs and rates, travel and subsistence. In support of your Proposal you are requested to provide clear details of all Dependencies, Assumptions, Risks and Exclusions that underpin your price.

Offer of Contract: *(to be completed and signed by the Contractor's Commercial or Contract Manager)*

Total Proposal Price in £	£951,580.81		(ex VAT)
Start Date:	October 4th 2021	**End Date:**	March 31st 2022

Lot Leads Representative	Name	[REDACTED UNDER FOIA EXEMPTION]
	Tel	[REDACTED UNDER FOIA EXEMPTION]
	Email	[REDACTED UNDER FOIA EXEMPTION]
	Date	September 21st 2021
Position in Company	Senior Consultant	
Signature	[REDACTED UNDER FOIA EXEMPTION]	

Core Work – Breakdown

Lot Lead Rates for Task Management Services (TMS)							
Team Member Name	**Role**	**Activity Type**	**Rate (£)**	**Total Hours**	**LMS recovery per role per hour ('d' element)**	**Total LMS recovery due (£) ('d' x total hours)**	**Total TMS Cost (£) (Rate x total hours)**
[REDACTED UNDER FOIA EXEMPTION]							

Work Delivered By Sub-Contractor(s)						
Name of Sub-Contractor	**Supplier Type**	**Activity Description**	**Team Member Role**	**Rate (£)**	**Total Hours**	**Total Cost (£)**

Work Delivered By Sub-Contractor(s)						
[REDACTED UNDER FOIA EXEMPTION]						

Travel, Subsistence, Materials & Equipment Travel & Subsistence					
Supplier Name	**Spend Type**	**Description / Rationale**	**Unit Cost (£)**	**Quantity**	**Total Cost (£)**
Materials & Equipment					
Supplier Name	**Spend Type**	**Description / Rationale**	**Unit Cost (£)**	**Quantity**	**Total Cost (£)**
[REDACTED UNDER FOIA EXEMPTION]					

Core Work – Milestone breakdown costs

Proposed Milestones Payments

Your TMS bid costs shall be included in milestone 1.

The final Milestone must reflect the actual cost of the deliverable, and be greater than 20% of the Task value, unless otherwise agreed with your Commercial POC

Please duplicate the template per milestone table format below as necessary, and rename milestone number accordingly.

Milestone M1						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**
Milestone M2						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**
Milestone M3						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M4						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M5						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M6						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M7						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M8						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M9						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M10						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M11						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M12						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M13						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M14						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**

Milestone M15						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**
			t			

Milestone M16						
Description	**TMS cost (£)**	**Self-Delivery cost (£)**	**Sub-contractor cost (£)**	**Total milestone cost (£)**	**Milestone due date**	**DEFCON**
[REDACTED UNDER FOIA EXEMPTION]						
		Total Cost (All Milestones)		**£951,580.81**		

Tasking Form Part 3:

To be completed by the Authority's Commercial Officer and copied to the Authority's Project Manager.

1. **Acceptance of Contract:**		
Authority's Commercial Officer	Name	[REDACTED UNDER FOIA EXEMPTION]
	Tel	[REDACTED UNDER FOIA EXEMPTION]
	Email	[REDACTED UNDER FOIA EXEMPTION]
	Date	30/09/2021
Requisition Number		1000166791
Contractor's Proposal Number		013235-95987L
Purchase Order Number		DSTLX-1000163301
Signature		[REDACTED UNDER FOIA EXEMPTION]
Please Note: Task authorisation to be issued by the Authority's Commercial Officer or Contract Manager. Any work carried out prior to authorisation is at the Contractor's own risk.		