RCloud Tasking Form – Part B: Statement of Requirement (SoR)

Reference Number	1000166799
Version Number	**0.1**
Date	**12/10/2021**

1.	**Requirement**
1.1	**Title**
	Automatic Jack
1.2	**Summary**
	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. Redacted under FOI Exemption
1.3	**Background**
	AUTOMATIC JACK has been looking at developing autonomous Redacted under FOI Exemption agents Redacted under FOI Exemption if developed further would be of significant benefit to the ARCD project.
1.4	**Requirement**

This activity will cover 12 months of software development effort.

Redacted under FOI Exemption

The ARCD project has a requirement to take forward the current AUTOMATIC JACK capability and fund the next phase of work to mature the capability and tailor it to meet the project's goals Redacted under FOI Exemption

This task will be managed using an Agile approach, where tasks will be prioritisation and managed via a backlog, accessible to the supplier and Dstl. Direction to the development team will be provided by the Dstl Technical Lead. The agile approach will develop high level epics for experimentation and delivery, such as the use of different reinforcement learning approaches, Redacted under FOI Exemption and potential integration into other Dstl owned toolsets. The tool should demonstrate the capability to progress towards generalisability Redacted under FOI Exemption

We have agreed with the prior funding authority that we will take AUTOMATIC JACK forward which will include scaling the Roke development team, setting the direction of travel and managing the prioritisation of tasks.

Specific Technical Requirements
The following list of tasks is not prioritised, but numbered for ease of reference:

1. Redacted under FOI Exemption
2. Further extend range of training Redacted under FOI Exemption
3. Capability enhancement (new actions) - extend repertoire of techniques Redacted under FOI Exemption
4. Redacted under FOI Exemption - Scalability of action and observation space
5. Redacted under FOI Exemption
6. Enhance the Reinforcement Learning algorithm library options – Stable Baselines 3 and Ray RLlib integration
7. Redacted under FOI Exemption
8. Explore Tuneable model behaviour Redacted under FOI Exemption
9. Investigate and Research solutions for key issues identified already such as how to deal with a scaling action and observation space. As well as other issues such as uncertainty
10. Overall DeveOps Enhancement – Make required engineering changes to support approaches and other epics.

Project Management

The supplier will manage delivery of the project and provide appropriate progress reports. Specifically, the supplier will be required to:

1) Host an initial start-up and planning meeting with the Authority. During this meeting, the Authority will discuss the project backlog and provide further information on how it intends to utilise and exploit the software developed through this activity. The outputs of this meeting will be captured in a set of minutes that will be delivered to the Authority.
2) Prepare and issue a Project Management Plan and provide this to Dstl for approval within 20 working days of contract award.
3) Produce bi-weekly progress reports for the Authority covering the status of development activities, risks, opportunities and issues related to delivery. These reports can be delivered via email.

Planning & Definition of User Stories

The supplier will work with the Authority to develop a plan for achieving the specific technical requirements.

The output should be a set of user stories/ epics, captured in a project backlog, which will be managed and maintained in line with the adopted agile development approach.

The project backlog will constitute a visible record of current and future progress towards achieving the overall aims of this activity. The Authority may alter the priority of tasks on the backlog following completion of development sprints, discussed below.

Software Development Environment

1) The supplier shall be responsible for providing an appropriate software development environment. If a teaming approach is employed, this environment should enable collaboration whilst mitigating issues associated with exposing Intellectual Property.

2) The supplier shall use git for software version control.

Software Development

The supplier shall conduct software development sprints over a period of 12 months. For each sprint, the supplier shall:

1) Attend a sprint planning meeting with the Authority to agree the sprint's goals and backlog items that will be addressed. Where practical, this meeting shall be hosted by the supplier. This can be done using video teleconference facilities. Whilst the duration of sprints will be determined in sprint planning meetings, it is anticipated that each sprint will be 2-4 weeks in duration and align with reporting requirements. Part of the sprint definition will be to identify and select any appropriate standards that software or data generated during the sprint must conform to. The sprint backlog will be reviewed and endorsed by the Authority prior to sprint commencement. Once the Sprint Backlog has been agreed, no changes to it can occur during the sprint unless agreed with the Authority.

2) Undertake software development activity to realise the aims of the sprint. Each sprint should deliver a Minimum Viable Product (MVP). Software shall be integrated, tested and documented in line with the requirements defined in the sprint planning phase. The Authority shall review proposed verification, validation and test procedures before sprint activity commences.

    a) Unless there is a language dependency imposed by activities, AUTOMATIC JACK shall be written in the Python programming language. General Python programming good practice (e.g. PEP8) and guidelines outlined in JSP 188 should be followed. Other software components should be written in Python where appropriate.

    b) The software must be able to run on a supported version of Ubuntu (>= Ubuntu 18.04 LTS) and without reliance on any closed-source, proprietary, software dependencies (unless specified by the Authority). Consultation with, and agreement from, the Authority is required prior to integrating any third-party software libraries to ensure that requirements for software licenses can be met.

    c) Unless there is a dependency due to integration with third party technologies, input and output data formats are to be non-proprietary (e.g. CSV or JSON), and must be documented. Use of any proprietary or closed data formats shall be agreed with the Authority.

    d) Source code shall be documented. The use of document generating tools, configured to populate documentation is encouraged.

    e) The supplier shall conduct and fully document all appropriate Verification and

Validation (V&V) of this software following industry best-practice (e.g. TickITplus). All software dependencies are to be documented, and distributed as part of the final deliverable (licenses permitting).

f) Any compiled binaries or compiled byte code delivered as part of this work are to be compliant with all third-party licensing conditions.

3) Attend a sprint review meeting, during which the supplier(s) will provide an overview of progress and demonstrate new software features developed during the sprint. Where practical, this meeting shall be hosted by the supplier. The outcomes of these review meetings should be captured in a short summary report, detailing the key outcomes of the sprint, which will be used by the Authority for internal progress and performance monitoring.

Software Delivery

The supplier shall:

1) Make the software source code available to the Authority throughout the contract period. This shall be achieved by using a private git repository (or repositories), hosted by the supplier and accessible over the Internet, following best practice for securing access to all parties. It is expected that the specific approach selected by the supplier will be confirmed in the proposal submitted in response to this requirement. The Authority requires access to 'weekly', unstable, source code increments, and post-sprint 'stable' builds for internal test and development purposes.

2) Provide code compilation instructions (where necessary).

3) Provide documentation that describes the design of the software in detail, including the underpinning algorithms; processes / control flow; technical design; etc.

4) On conclusion of the project, provide source code and any compiled byte-code files to the Authority.

Project Conclusion and Close-Down

At the end of the project, the supplier shall;

1. Provide a summary document that describes the functionality of tool. This is intended to be shared with MOD and wider government stakeholders, Redacted under FOI Exemption
2. Provide a summary brief and software demonstration to the customer and stakeholder community. Invitations to this event will be managed by the Authority.
3. Attend a project close-down meeting. The supplier shall provide a brief summary of activity on the project, identify relevant lessons for the Authority.
4. Provide the Authority with a copy of the latest version of the project backlog, detailing any extant user stories.

Security Requirements

The classification of the work will start at Official. But will be assessed as it continues. The classification could increase to Official-Sensitive and then potentially to Secret. Therefore, the supplier (Roke) will be required to have SC Cleared staff working on this task.

Intellectual Property Requirements

All software components and documentation relating to AUTOMATIC JACK shall be delivered under DEFCON 705 Full Rights.

	Key Outcomes Key outcomes of this task are: • An end of project demonstration event to the Authority and broader stakeholder community • Software source code and (where necessary), compiled binary software, for all components of the AUTOMATIC JACK tool • Sprint progress reports • Project backlog • Epic Completion Summary Reports • End of Project Report
1.5	**Options or follow on work** *(if none, write 'Not applicable')*
	Any follow on work offered is dependent on both confirmation of funding and an appetite from the project team to take the outputs from these task forward.

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	2 Weekly Sprint Progress and Technical Updates	T0+1 Months	Presentation (.pptx)	n/a	O	Presentation pack shall include (but is not limited to): • Update on technical progress • Progress report against project schedule. • Review of risk management plan. • Commercial aspects. • Review of deliverables. • Risks/issues.	DEFCON 705 Full Rights
D - 2	Summary Document		Report		O	An overview of functionality of the tool, and how this was achieved.	DEFCON 705 Full Rights
D - 3	Demonstration event		Demonstration		O	End of project capability demonstration to stakeholders	DEFCON 705 Full Rights

D - 4	Software Source Code		Version controlled source code files		O	Shall include all source code generated in support of the task as both a weekly unstable build and a monthly stable build.	DEFCON 705 shall apply to source code and associated supplementary tools
D - 5	Software Executable Code		Software Executables		O	Where necessary, this shall include all executable code (or compiled byte code) and files required to run the software, as both a weekly unstable build and a monthly stable build.	DEFCON 705 shall apply to source code and associated supplementary tools
D - 6	Software Documentation		Report(s)		O	This shall describe the design of the software in detail, including the underpinning theory and equations; processes / control flow; technical design; data specifications etc. The technical detail shall be sufficient to permit independent reproduction of the system.	DEFCON 705 Full Rights
D - 7	Project Backlog				O	This shall define project epics and user stories for extant development items.	DEFCON 705 Full Rights

***Technology Readiness Level required**

Notes- IPR should be inserted / checked by commercial staff before sharing with the supplier(s) to ensure accuracy.

1.7	**Standard Deliverable Acceptance Criteria**

This could be 'as per Framework T&C's' once an appropriate framework is later confirmed (links to section 13 of RCA). Consider the timeframe for our review of deliverable(s) (acceptance/rejection).

- All reports and outputs must address the requirement as stated in Section 1.4 of this SOR.
- 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.
- 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.
- All Reports shall be free from spelling and grammatical errors and shall be set out in accordance with the Statement of Requirement (1) above.

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

1.8	**Specific Deliverable Acceptance Criteria**

	Product	**Acceptance criteria**
1.	Kick-off Meeting Minutes	Shall provide a record of discussions of the kick off meeting. Shall be delivered as both a Microsoft Word (.docx) and Portable Document Format (PDF) (.pdf) document. Review from Dstl project team. Acceptance period: 5 working days
2.	Sprint Summary Reports	Shall summarise (not detail) the key outcomes of the sprint. These reports shall be delivered as both a Microsoft Office (e.g. .pptx, .docx as appropriate) and PDF (.pdf) document, and must and include the Authority Release Documentation Page (RDP). Review from Dstl project team.

		Acceptance period: 5 working days
3.	Source Code	Shall include all source code generated in support of this task. Review from Dstl project team. Acceptance period: 10 working days
4.	Software executable code	Shall include all executable code (or compiled byte code) and files required to run the AUTOMATIC JACK software. Review from Dstl project team. Acceptance period: 10 working days
5.	Project Documentation	Shall describe the design of the AUTOMATIC JACK software in detail, including the underpinning theory and equations; processes / control flow; technical design; etc. The technical detail shall be sufficient to permit independent reproduction of the system. These documents shall be delivered as both a Microsoft Word (.docx) and PDF (.pdf) document, and must and include the Authority Release Documentation Page (RDP). Review from Dstl project team. Acceptance period: 10 working days
6.	Project Backlog	Shall define project epics and user stories for extant development items. Review from Dstl project team. The backlog shall be provided in Microsoft Excel (.xlsx) format. Review from Dstl project team. Acceptance period: 10 working days
7.	Demonstration Materials	All draft presentations materials must be delivered in Microsoft Office formats (e.g. .docx, .pptx) to aid reviewing by the Authority Technical Partner (TP). Final material must be in both Microsoft Office and PDF format and include the Authority Release Documentation Page (RDP). The supplier(s) should record the final demonstration. Recordings should be in an open video format that is playable through the VLC media player. Review from Dstl project team. Acceptance period: 10 working days

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 below)
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	UK SECRET
	Of the Deliverables/ Output	UK SECRET
3.2	Security Aspects Letter (SAL)	
	Yes If yes, please see SAL reference- 1000166799	
3.3	Cyber Risk Level	
	Not applicable	
3.4	Cyber Risk Assessment (RA) Reference	
	570119745	

4.	Government Furnished Assets (GFA)

No

5.	Proposal Evaluation criteria
5.1	Technical Evaluation Criteria
5.2	Commercial Evaluation Criteria