Statement of Requirement (SoR)

Reference Number	**1000168617**
Version Number	**0.1**
Date	**04/10/2021**

1.	**Requirement**
1.1	**Title**
	Python Developers to Support the Autonomous Resilient Cyber Defence (ARCD) Project

1.2	**Summary**
	The Autonomous Resilient Cyber Defence (ARCD) project aims to develop self-defending, self-recovering concepts for military platforms and technologies. The project is seeking a team of Python developers to: contribute to the development of the Cyber Autonomy Gym for Experimentation (CAGE), a 5-eyes initiative under The Technical Corporation Program (TTCP); provide software engineering support to an internal Dstl project team reviewing and assessing emerging open source reinforcement learning tools. The project team will work to provide the outputs and deliverables set out in section 1.6 below, and will be required to work collaboratively with Dstl staff, often on the Dstl floorplate (depending on COVID-19 guidance). Candidates should have a strong understanding of machine learning, deep learning and generative approaches. Candidates must be able to quickly understand the problems, develop suitable sprint plans, proactively seek feedback from relevant internal experts and work independently to carry out development, research and evaluation. Dstl would welcome teaming and/or suppliers working with SMEs to deliver this requirement, however this is not mandatory.
1.3	**Background**
	The CAGE project aims to provide a platform for development and validation of autonomous, Artificial Intelligence (AI) driven agents for cyber defence. The scope of work on CAGE includes (but is not limited to): implementation of a state space visualisation capability for the CAGE simulator; expanding the scope of the Action Set for the CAGE simulator; and implementation of specific agents within the CAGE framework. The supplier will be required to document their progress and brief the Dstl project team (and international partners) on progress. The CAGE project has been running since the start of 2020 and is currently exploring the development of environments in which to train AI-based intelligent agents. This work will continue over until 2023.

	The scope of software engineering support to the Dstl project team will include (but is not limited to): identification, assessment and documentation of new and emerging reinforcement learning tools for cyber security; supporting the development of abstract and emulated cyber security reinforcement learning environments, which can be shared with Industry and Academia; and development of common libraries and tools to support reinforcement learning research activities.
1.4	**Requirement**

	Dstl has a requirement for a team working on the floorplate to support ARCD. The potential scope of the requirements are considerable, so the supplier must demonstrate that the personnel they are proposing to provide are: • Highly skilled in the Application of Artificial Intelligence (AI) and Machine Learning (ML) techniques with a focus on both Reinforcement Learning and Deep Reinforcement Learning. It is anticipated that capacity will be provided by individuals at and above Senior Engineer/Scientist grade. • Experienced in debugging methodologies for simulations as well as Reinforcement Learning environments. • Able to propose new AI/ML solutions for investigation, applying AI/ML techniques to Cyber Defence, and develop suitable work plans. • Able to proactively seek feedback from relevant internal experts • Able to independently to carry out research and evaluation. • Experienced with the Python 3 software language, Jupyter notebooks (or similar) and are able to apply good software practices (i.e. code documentation, testing and validation) • Good communicators and are able to work with the team and stakeholders. Personnel will be expected to write work plans for specific tasks, technical memorandums on completion of each investigation and a summary report at the end of the phases. This work is being contracted based on capacity, not the contracting of named individuals. If the individuals that are providing the capacity do not meet the requirement (either through not adequately meeting the competencies as set out in this SOR, or the nature or understanding of the project changes), it is expected that the Supplier shall take steps to rectify the issue (e.g. by rotating team members). Dstl would welcome teaming and/or suppliers working with SMEs to deliver this requirement, however this is not mandatory. REDACTED – SENSITIVE INFORMATION The supplier will be working collaboratively with both an internal Dstl team and international partners based in Australia and the US West Coast. All work must be conducted on Dstl accredited infrastructure on the appropriately classified network.

	Personnel will be supervised by the ARCD Project Technical Authority (PTA) and Project Manager. **Approach:** Work conducted collaboratively with Dstl staff shall be managed in an Agile manner using the Kanban approach and a prioritised backlog hosted on Dstl's internal Jira. This backlog of tasks shall be developed and managed by the supplier aligned with the high-level tasks outlined in this SoR. The work conducted with international partners shall be conducted using the DI2E platform provided by the US. The DI2E platform shall be used as the central code repository with developers from each country will pick up specific features and develop them locally before pushing back to the central repository. Work will be monitored through the following: • Monthly meetings covering Sprint Review and Planning will be setup between the contractors and the relevant Dstl personnel to review current progress and prioritise the next month's work. This will be conducted at Dstl Porton Down if required to support increased engagement, planning and idea sharing. • The Supplier shall prepare fortnightly progress presentations for discussion at these sessions covering the work completed to date, any issues/blockers as well as potential additional requirements identified during the previous period. • Additionally monthly PM reporting on spend to date and forecast will be required. • The Supplier shall prepare and deliver an end of phase summary report and presentation covering a summary of all tasks completed to date, lessons identified and potential future requirements. Whilst certain aspects of work may be conducted remotely, it is essential that the supplier provide capacity that is available to work on the Dstl Porton Down floorplate for a minimum of 3 days per week (ideally more). All work completed as part of this project will be delivered under DEFCON 703. Initially, work will focus on:

	• Requirement 1: Supporting the development of CAGE alongside international partners using the DI2E platform
	  ○ Requirement 1.1: Implement State Visualisation for the CAGE Simulator
	  The current CAGE simulation framework does not currently have a good method of tracking simulation runs as they progress visually. This requirement will look to implement a method of displaying the current system state such as host state and actions performed by the agents.
	  ○ Requirement 1.2: Implement a Broadened Action Set for the CAGE Simulator
	  The current CAGE simulation framework has limited actions for both Blue and Red agents. This requirement will look to increase this area such as adding the feature to add a simulation component for malicious network traffic.
	  ○ Requirement 1.3: Implement both Static and Algorithm Driven agents for the CAGE Simulator
	  The current CAGE simulation framework has a number of static and algorithm driven agents. As the number of scenarios and environments increases, there will be a requirement to train and refine both Blue and Red agents to act as opposition.
	  ○ Requirement 1.4: Documenting and Briefing the wider Dstl team progress on CAGE
	  This requirement will be focused on documenting progress of CAGE development and ensuring the wider Dstl team are kept up to date. This will help with understanding what is being learnt and how it can support and shape future work.
	• Requirement 2: Identification, Assessment and Documentation for new and emerging Reinforcement Learning for Cyber Security Tools
	This requirement is focused on identifying potential open source technology, setting them up, assessing the tools quality and applicability to our aims and then documenting what was found.

	• Requirement 3: Supporting the development of highly abstract cyber security reinforcement learning environments, which can be shared with Industry and Academia to begin thinking above how Reinforcement Learning can be used in Cyber Security. This requirement would be focused on enhancing the overall suite of environments and adding functionality such as environment randomisation, in-depth logging as well as multi-agent support. • Requirement 4: Technically Assuring and Reviewing ARCD Software deliverables The wider ARCD project is procuring a range of software deliverables and this task would be focused on providing third party technical assurance of the deliverables alongside the ARCD technical partner/Project Technical Authority. Work may continue on the topics as above if there is additional research needed. Potential additional areas identified are: • Requirement 5: Development of environments and extending/integrating delivered software The wider ARCD project will be procuring a range of software deliverables. This task is focused on supporting integration of common and complimentary tools. • Requirement 6: Contribution to Open Source projects on Dstl's Behalf This task would be focused on contributing code to open source projects to add functionality Dstl requires. • Requirement 7: Development of common libraries and tools to support Reinforcement Learning Research This requirement would be focused on developing the "glue" which would be used by Dstl, our partners and suppliers to share results, agents and environments.
	Options or follow on work

	Potentially the work could continue for a further 6 -12 months, which would be placed as a new task. This would be dependent on the successful outcome of the previous 12 months, and is subject to contract.

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	Project kick off meeting	T0+1w	Email minutes of meeting.	n/a	REDACTED – SENSITIVE INFOMATION	Attendance at meeting Introduction of self and relevant background work Agreement on ways of working and communications Review and agreement for plan to meet initial requirements. Review of any data sets and comments to Dstl. Minutes of meetings.	As per DOS 5 Terms

D2	Attendance at monthly sprint kick off meetings and plan for the month	Monthly – on agreed week	email	n/a	REDACTED – SENSITIVE INFOMATION	Attendance at Dstl Porton Down Bullet point plan of work agreed emailed to work package leads, PM and PTA for review and approval.	As per DOS 5 Terms
D3	Technical Sprint Reporting	Monthly – on agreed week	Attendance and Dstl site. Powerpoint + Jupyter notebook	n/a	REDACTED – SENSITIVE INFOMATION	Attendance at Dstl Porton Down, preparation and delivery of presentation and demo of: work undertaken in sprint, findings, and recommendations.	As per DOS 5 Terms
D4	Monthly contractor reporting	Monthly following the end of the month	Email	n/a	REDACTED – SENSITIVE INFOMATION	Summary to include but not limited to: • Spend to date against forecast. • Status of deliverables. • GFA and Dependencies • Risks, Issues etc • Supplier performance.	As per DOS 5 Terms

D5	Technical Memos	Completion of each Requirement	Microsoft Word	n/a	REDACTED – SENSITIVE INFOMATIO N	On completion of each requirement, a technical memo shall be written detailing what has been examined, the results and any conclusions and recommendations. These may be produced independently or in conjunction with other Dstl researchers.	As per DOS 5 Terms
D6	Final summary report and presentation	25th November 2022	Presentation in Microsoft powerpoint. Report in word.			**Report**: Successful technical work and output, as well as Any areas of work that could not progress and why. To include a 2 page executive summary for non-technical stakeholders. **Presentation**: Summary presentation of the report to Dstl and potentially for stakeholders.	As per DOS 5 Terms
D7	Software source code	Duration				All code should be fully commented and uploaded to the relevant Source Code Management (SCM) infrastructure, with evidence of testing and validation undertaken. Code should be written in	As per DOS 5 Terms

		At a minimum, monthly/end of each phase				Python and may make use of interactive Jupyter notebooks. Discussion on licencing of open source software and highlight if it is not permissive.	

*__Technology Readiness Level required__

1.7	**Standard Deliverable Acceptance Criteria**
	•
1.8	**Specific Deliverable Acceptance Criteria**
	Software acceptance criteria • All code shall follow Dstl processes and procedures, including input to a Software Project Management Plan (SPMP). • All code should be fully commented and uploaded to the appropriate SCM infrastructure, with evidence of testing and validation undertaken. • All completed code must be validated according to the methodology indicated in the SPMP and recorded in documentation. **Written work acceptance criteria** • Written work shall be reviewed by the Dstl WPL, PTA, PM, and LTR. • Shall be written in good English, and free of spelling and grammar issues. • Shall cover the full scope of the requirement, and shall provide a clear technical narrative. • Shall conform to Athena report writing guidelines and formats.

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	REDACTED – SENSITIVE INFOMATION
	Of the Deliverables/ Output	REDACTED – SENSITIVE INFOMATION
3.2	**Security Aspects Letter (SAL)**	
	REDACTED – SENSITIVE INFOMATION	
3.3	**Cyber Risk Level**	
	REDACTED – SENSITIVE INFOMATION	
3.4	**Cyber Risk Assessment (RAF) Reference**	
	REDACTED – SENSITIVE INFOMATION	

4.	Government Furnished Assets (GFA)

GFA to be Issued - Yes

GFA No.	Unique Identifier/ Serial No	Description:	Available Date	Issued by	Return Date or Disposal Date (T0+)
GFA-1		Dstl laptop per staff member	At start of contract	Dstl	At end of contract

5.	Proposal Evaluation criteria
5.1	Technical Evaluation Criteria

	Technical evaluation criteria (60%) (weightings of each criteria are shown in brackets below): • Demonstrate with evidence the ability to quickly familiarise with a complex inherited codebase. (0.2) • Demonstrate expertise and experience of developing software to implement machine learning and AI algorithms. (0.2) • Demonstrate expertise and experience of evaluating and testing machine learning and AI systems and tools. (0.2) • Demonstrate experience of developing software in the context of the cyber security domain. (0.2) • Provide a breakdown of the team structure (please include CVs of the team members doing the work). (0.2) Cultural fit criteria (20%) (weightings of each criteria are shown in brackets below): • Demonstrate with evidence ability to follow industry best practice throughout the whole software development lifecycle, from requirements gathering through to documentation, testing, verification and validation (including examples of tool chains used). (0.2) • Demonstrate consistent cultural commitment to agile software development practices. (0.2) • Demonstrable experience of working collaboratively with external organisations to realise project goals, and responding to evolving requirements. Show evidence of being transparent and collaborative both internally and with the customer when making decisions. (0.2) • Show evidence of an internal culture of knowledge and experience sharing. (0.2) • Follow industry best practice when conducting Verification and Validation for example TickITplus. (0.1) • Demonstrate ability to successfully deliver within the UK government customers. (0.1)