Dstl R-Cloud
Commercial Services
Porton Down
Salisbury
Wiltshire
SP4 0JQ

E-mail: dstlrcloud@dstl.gov.uk

Statement of Requirement for the R-Cloud Cyber Strategic Capability

Introduction:

The Defence Science and Technology Laboratory (Dstl), which is part of the UK Ministry of Defence (MOD), is refreshing its commercial agreement for Science and Technology (S&T) research contracts, known as R-Cloud (Research Cloud).
MOD places extensive fundamental, experimental and applied research with industry and academic suppliers and wants to broaden access for this supply base, reducing the cost of trading with MOD and enabling agile contracting. R-Cloud complements MOD's other contracting mechanisms and academic and industry suppliers of S&T research are now invited to apply to join MOD's research supplier community within the Cyber Strategic Capability.

This statement of requirement relates to suppliers joining R-Cloud within the Cyber capability area. R-Cloud provides a low barrier to entry for potential suppliers and offers direct access to MOD's current and future research requirements. Academic and industrial suppliers of Cyber research are invited to apply to R-Cloud if you are a supplier of Science and Technology Research in this area.

Cyber encompasses a broad range of technical areas with our strategic capability focused around the **Cyber Resilience, including safety,** of systems and platforms and understanding the impact of events in cyber-space to enable decision makers to decide and act appropriately. Skill sets include those drawn from the fields of Human Sciences, Systems Characterisation and Systems Dependability, through to Software, Complex Electronic Hardware, Radio Frequency and Electronic Technologies, and Algorithms, Data and Protocol Analysis.

Below is a summary of overarching cyber research requirements.

Cyber Resilience of MOD Platforms and Systems

MOD needs to have assurance that its systems and platforms are secure against attacks from cyberspace so that it can maintain freedom of manoeuvre and operate independently of any enemy actions. It also requires assurance that safety risks are tolerable and As Low As Reasonably Practicable (ALARP).

This combination requires research into the security and vulnerabilities of a broad range of socio-technical systems comprised of embedded devices, protocols and networks that reach far beyond those of traditional desktop Information Communications Technology (ICT). It also

requires research into emergent properties of complex systems, including the bounded predictability of programmable behaviour.

The scope of coverage of topics related to Cyber Resilience includes, but is not limited to, the following:

a) Technologies, processes, standards and policy associated with cyber security, system safety and programmable element safety.

b) System engineering approaches to cyber resilience to assess and test reliability, dependability, resilience and security, and to determine potential vulnerabilities in socio-technical systems. Management of emergent properties, like safety and resilience, is an important aspect.

c) Tools, methods and processes to analyse, assess and test the cyber resilience, dependability or reliability of complex electronic hardware and software. This includes bespoke software, firmware and embedded hardware, as well as other more general forms of ICT. The role of data is also explicitly included.

d) Tools, methods and processes to analyse, assess and test cyber resilience, dependability or reliability of wired and wireless communications systems, networks and protocols. This includes closed, bespoke networks and protocols as well as those using open standards commonly found in cyber-space.

e) Tools, methods and processes to provide assurance of the behaviour of artificial intelligence, including (but not limited to) that developed using machine learning techniques. This includes both the artificial intelligence component, as well as wider system-level enabling architectures.

f) Machine learning and human machine hybrid technologies to automate and expedite decision making and to reduce the problem spaces presented by the challenges to allow talent to focus on areas where human ingenuity and creativity are best applied is flagged.

g) Pan-Defence Lines of Development (DLOD) approaches to improve cyber resilience including changes to concepts, doctrine, and training.

This may include, but is not limited to:

- Basic research into processes, techniques and technologies that may be of use to Cyber Resilience.
- Applied research into component, sub-system, system and systems of systems level aspects of socio-technical systems that provide Cyber Resilience.
- Horizon scanning to identify new processes, techniques and technologies that may be of use to Cyber Resilience.
- Software and hardware tools to analyse assess and test hardware, firmware, software and protocols. This may include wired and wireless systems that do not conform to openly published standards and so includes waveform design, generation, reception and evaluation.
- Tools to undertake ‘what-if’ analysis to test Cyber Resilience options.
- Upgrades for current UK MOD platforms, systems and doctrine.