Statement of Requirement (SoR)

Reference Number	**RQ0000014041**
Version Number	**1.0**
Date	**02/08/2022**

1.	**Requirement**
1.1	**Title**
	Discovery Cloud environment
1.2	**Summary**
	Dstl has a requirement for an accredited and approved Redacted under FOIA Section 24 - National Security cloud environment accessible to users on Dstl DONB and MODNET, with secure two way Redacted under FOIA Section 24 - National Security data connections to Dstl and MOD networks and internet connectivity. The purpose of the environment is to host applications procured or developed for Horizon Scanning and technology watch. Dstl require a fully managed and supported service. The supplier shall load the environment with specified existing applications, enable continuous development and deployment of new applications, including by third party suppliers under separate contract to Dstl, and shall ensure it is scalable to ensure responsiveness for data processing and for user interaction. Before the end of the contract the supplier shall migrate the contents of the environment to MODcloud and verify correct functionality.
1.3	**Background**

This work is part of Dstl’s Discovery project. Its vision is: *“Defence has a best in class software system to allow users to find, explore, summarise and investigate areas of emerging Science and Technology worldwide”.* The project objectives are:

1. Find, trial and secure off the shelf products and data to build short term horizon scanning and technology watch capability.
2. Develop and deploy a software platform to provide Science and Technology Intelligence and integrated knowledge management capability for the long term.
3. Research to ways to augment and automate the futures pipeline, in particular horizon scanning.

There are three key milestones for the project:

- July 2022 – *Minimal Viable Capability (MVC)*: Stand-alone applications (Objective 1) at OFFICAL
- July 2023 – *Initial Operating capability (IOC)*: First version of integrated platform (Objective 2), plus Stand-alone applications, at Redacted under FOIA Section 24 - National Security
- July 2024 – *Full Operating Capability (FOC)*: Updated version of integrated platform, incorporating automation and research outputs (Objective 2, 3) at Redacted under FOIA Section 24 - National Security

Use of MVC, IOC and FOC in this SOR refer to these project milestones, not milestones for the cloud environment. The cloud environment that will be delivered by the work described in this SOR support will be the Redacted under FOIA Section 24 - National Security location that the standalone applications and integrated platform will be developed, deployed and used. Redacted under FOIA Section 24 - Nationa capability is a stretch goal for FOC, but formally is not required at this stage.

Policy is changing so that MODcloud will be the mandated first choice of environment for all MOD applications in the cloud. In May 2022, this project received approval to use an outsourced cloud solution to mitigate technical and business risks to schedule as MODcloud stands-up. The approval was subject to a guaranteed transition to MODcloud by the supplier who completes the work.

1.4 Requirement

1. The supplier shall provide a managed cloud service which includes:

- A ‘discovery’ phase where the supplier determines the detailed technical requirements working with the Authority and the Authorities suppliers
- Definition of the cloud system including tools, techniques and processes

- UK MOD Accreditation to Redacted under FOIA Section 24 - National Security including completion and application of all necessary processes and direct engagement with accreditation authorities
- Environment maintenance to keep the environment up to date with MOD policy and security requirements
- A fully supported end-to-end managed service with service support throughout the operational life
- Access to the environment at any time
- Standard Recovery Time Objective (RTO) and Recovery Point Objective (RPO) times
- The supplier loading, testing and verifying functionality of applications listed in this statement of requirement, working with third party providers as necessary
- The supplier working with and enabling a third party company or companies under separate contract to the Authority to develop new applications to be hosted on the environment. This may include requirements that change the configuration of the environment
- A configuration that easily, rapidly and if necessary automatically adjustable and scalable within reasonable bounds
- Migration to a MODcloud hosted environment as soon as possible and by the end of the contract at the latest.

2. The supplier shall deliver a cloud environment that meets the high level requirements outlined in this section. The detailed technical requirements shall be generated by the supplier in an initial discovery phase.

2.1 System and technology

- Enabling architecture shall be defined
- Dstl has a preference but not confined to Amazon Web Services (AWS) for hosting of data and applications
- The environment must support DevOps: both development, production and continuous integration

2.2 Users

- A user base of DSTL, wider MOD, and Cross-Government partners, and industry/academia
- Users shall comprise Application Users and Developers

- Day 1 User Pool: Up to 100 users comprising 50 DSTL users, 10-20 wider MOD, plus developers from suppliers
- 25% Day 1 user concurrency
- Users shall access the environment using existing devices, for example DSTL provisioned laptops or MODNet devices via web browsers
- Identity and Access Management (IdAM) shall be used so Dstl and MOD Users can access the system with their existing Dstl or MOD accounts.
- Secure third party (industry/academia) shall be able to access the environment without Dstl or MOD accounts is required.

2.3 Connectivity

- Access to applications within environment via a web browser is required for Application Users. Dstl and MOD application users shall not need to go through a virtual desktop or another intermediary process to reach applications.
- Redacted under FOIA Section 24 - National Security
- Connectivity to the existing Redacted under FOIA Section 24 - National Security network is required. The supplier will be responsible for technical discussion and enabling agreements.
- Connectivity to the existing Redacted under FOIA Section 24 - National Security network is required. The supplier will be responsible for technical discussion and enabling agreements.
- RLI connectivity, if assessed as appropriate and necessary by the supplier shall be provided.

Connectivity use cases are:

- Dstl developers shall connect to develop, test and deploy code
- Redacted under FOIA Section 24 - National Security
- Industry suppliers shall connect to maintain their applications
- Redacted under FOIA Section 24 - National Security
  Redacted under FOIA Section 24 - National Security
- Industry suppliers shall be able to manual import and export of data up to Redacted under FOIA Section 24 - National Secu

- Redacted under FOIA Section 24 - National Security

Redacted under FOIA Section 24 - National S

- A backend connection between applications on the environment to Dstl network is required to scan/sync/ingest data daily
- A backend connection between applications on the environment to MODNet to scan/sync/ingest knowledge, daily, including files stored in SharePoint is required
- A backend data connection from applications on the environment is required to consume data from the internet and online applications (principally via HTTP and HTTP based APIs)
- A backend connection from applications on the environment is required to push data to the Dstl network daily
- A backend data connection from applications on the environment to export data to the internet applications via API in a controlled manner is desirable

2.4 Applications

There will be two main phases of application deployment in the Discovery project that is placing this requirement:

- ***Minimal Viable Capability* applications.** The supplier shall make these applications available on the cloud environment as soon as possible. The applications are Redacted under FOIA Section 24 - National Security shall be loaded on the environment in this phase subject to agreement of the application provider.

  We do not anticipate hosting an instance of the Redacted under FOIA Section 24 - National Securi in the environment. Applications within the platform require will access to data in Redacted under FOIA Section 24 - National Sec held externally. This must be accessible via API.

  Individual requirements for applications to be hosted in the environment are summarised in Table 1 at the end of this section. Connectivity requirements are summarised in Table 2.

All MVC applications will be subject to continuous development from the outset and the environment must be set up to enable this.

- **Project *Initial Operating capability* applications**

  Dstl intend place a separate contract for a supplier to undertake integration and development activity to build middleware that integrates the MVC applications, and create a new application in its own right to host new algorithms separately being developed.

  This phase is likely to include initially:

  a. A higher level of processing and analytics using Redacted under FOIA Section 24 - National Se
  b. Semantic search, which may be provided by a new 3rd party supplier
  c. Content management, which may be provided by a new 3rd party supplier
  d. Batch processing tasks in the new application which need to run routinely and have higher memory requirements

  The final integrated system requirements are expected to become more stretching. They will likely include some sort of document summarization and machine learning models that have the potential to be extremely computationally expensive. Connections to multiple other web endpoints for additional third party content will likely be required. The cloud environment shall be created to scale and be re-configurable to accommodate these requirements, which cannot be further defined at this time.

  Additional 3rd party applications, to be determined in a not-yet started trial phase may also be required. These will be a similar general nature to the specified applications; they will be knowledge based platforms for discovery and processing of data about science and technology that fill gaps in the specified application suite. The supplier is required to support their deployment, and retirement of any of the applications specified in this SOR that are no longer required.

3. Development and production

The environment shall support running of development code and applications in environment, in a controlled manner, and stable production version applications for end users. Appropriate mechanisms shall be put in place to enable deployment of new versions with minimal user disruption and to ensure accreditation in maintained via sufficient testing and compliance to relevant MOD processes.

A single data set should be used for both environments, although the ability to host test data sets exclusively for development is required.

4. Support, training, and documentation

The supplier shall provide support to the Authority and third party suppliers. This will include but not be limited to general use, deployment of new applications, deployment of new components, technical support and advice including to third party suppliers. Such support shall be provided throughout the contract.

Training in adoption of efficient working practices, tools and test regimes for continuous integration/continuous delivery shall be provided. Training is required as the environment reaches its early life support milestone and before the environment reaches Full Operational capability.

Technical system documentation and user documentation must be produced before the environment reaches Full Operational Capability.

5. Migration to MODcloud

The supplier shall migrate the environment and all applications to a MODcloud hosted environment by the end of the contract. Migration activity shall occur as early as possible which could be from the outset if feasible without jeopardising required timelines to a live and accredited system. The supplier shall create a migration plan, which could be delivered as part of the initial proposal.

6. Pricing and payment mechanisms

Where compute requirements scale up, in particular for batch processing, and for as yet unknown technical specifications associated integration, a mechanism to pay in proportion to usage is required in order to ensure core costs for the environment are reasonable and represent value for money throughout the contract life.

It is desirable that all payment is between Dstl and the supplier only and that subcontractor payment is managed by the supplier. It is understood that this may not be possible for MODcloud; Dstl also currently has no working mechanism to pay for

MODcloud directly. The supplier is required to consider the following options in order to achieve the earliest possible migration:

- Setting up a new payment mechanism between the supplier and the relevant subcontractors;
- MOD (not Dstl) paying directly, which may be possible but subject to administrative activity to reduce funding from Dstl's customers and reallocate to pay the supplier directly;
- Waiting until Dstl can pay directly, which could be January 2023 at the earliest but subject to risk as business agreements and payment systems are not in place.

Table 1: Overview technical requirements for initial applications (minimal viable capability)

These requirements are based on existing deployments of applications. They represent the systems to enable multiple users to access the environments at scale unless otherwise stated.

Redacted under FOIA Section 24 - National Security To be hosted in environment	1 x AWS RDS t3.small+ (2GB+ of memory and 1+ cores) running PostgreSQL Several x AWS EC2 r5.large or better (16GB+ memory, 2+ cores) running Ubuntu Linux S3 bucket; IAM user with bucket read/write access Data processing servers to be deployed either statically or dynamically as part of the AWS AutoScalingGroup.
Redacted under FOIA Section 24 - National Security To be hosted in environment	Training takes less than 24 hours use of ml.r5.12xlarge. 48 vCPU, 384 GiB, every month S3 bucket 5GB Requires Neo4j, PostgresDB In development, has not been yet deployed to users.
Redacted under FOIA Section 24 - National Security To be hosted in environment	Currently runs on individual user laptops (4 core, minimal storage 16GB memory), using R. Shall be moved to R Shiny server in the environment to serve multiple users. Relies on a live connection to Redacted under FOIA Section 24 - National Security hosted on the Redacted under FOIA Section 24 - National Secur API calls to Jive, Mediawiki and SharePoint systems). May also potentially need access to file shares, or replication of data (1.3 TB).

Redacted under FOIA Section 24 - National Security To be hosted in environment	CPU – Can run on 2 x Intel Xeon Platinum 8168 CPU @ 2.70GHz. 4 core preferable. RAM – 8MB, storage up to 80GB ElasticSearch currently 7.4.2, moving to 8.2, OrientDB currently 3.0.24 moving to 3.2.7, Apache Tomcat v9.0.33, JDK – 11, Angular 12, moving to 13. The application roadmap has plans to dockerise the application or move to a Linux VM. Replacements for ElasticSearch and OrientDB are being considered. Options on AWS include OpenSearch and Neptune respectively.
Redacted under FOIA Section 24 - National Security To be hosted in environment *subject to agreement from provider*	The current production environment for this application consists of: 7 x server with 1 core, 25 GB storage, 1 GB memory 7 x server with 2 cores, 80 GB storage, 4GB memory 4 x server with 4 cores, up to 200 GB storage, 8 GB memory 4 x server with 6 cores, 320 GB storage, 16 GB memory It is anticipated that a separate instance independently hosted could be scaled down.

Total data storage is estimated to be less than 10TB.

GPU is currently not a requirement for any applications.

Redacted under FOIA Section 24 - National Security needs enough access to the infrastructure to maintain and deploy an instance Redacted under FOIA Section 24 - National S They need at a minimum system administration/root access on Redacted under FOIA Section 24 - National Security usually a development tier along with the possibility of screen sharing to support troubleshooting/deployment on the other instances; or for maximum access have that same admin/root access for all tiers/instances used.

Dstl view it as likely that the environment will be used to host both Dstl private data and Redacted under FOIA Section 24 - National Security If it is possible to retain Redacted under FOIA Section 24 - National Security externally on a private Dstl instance, and retain accreditation, this is an option. The supplier is required to work this though with Redacted under FOIA Section 24 - National Sec to determine the best solution. If external hosting is used, this may need to change on-environment when integration activity begins.

Table 2: Connectivity requirements for initial applications

Redacted under FOIA Section 24 - National Security To be hosted in environment	TCP port 22 for SSH access (remote management, from specific IPs) TCP port 80 for HTTP access TCP port 443 for HTTPS access TCP port 6443 for kubectl (remote management, from specific IPs)
Redacted under FOIA Section 24 - National Security To be hosted in environment	Routine access to internet to ingest new data (e.g. nightly). Web access for users, with ability to manually export data to Redacted under FOIA Section 24 - National Security Eventually live with be required to other data and applications
Redacted under FOIA Section 24 - National Security To be hosted in environment	Highly dependent on real time connection to Redacted under FOIA . API calls to Jive, MediaWiki and Sharepoint systems. Approval to pass these requests to/from the Dstl network essential. Must be able to handle multiple API calls to different Dstl resources in parallel and return the results within 10 seconds. Each search requires 6 API calls. Internet access required
Redacted under FOIA Section 24 - National Security To be hosted in environment	Web service port (80, 443). Email port. Active Directory. No backend access to data stored on an accredited network, manual import of data via web only. Will eventually need connectivity to other applications in environment.
Redacted under FOIA Section 24 - National Security To be hosted in environment *subject to agreement from provider*	Web connectivity, low bandwidth. If hosted in environment, a backend inward connection from internet to futures platform servers is required to sync data. If not in environment, there is an eventual requirement to routinely export data to this platform. Eventual connection to other applications within platform for import and export of data.

1.5 Options or follow on work

	Option 1 – To be costed with initial proposal. Extend the service for 1 year. This option may be taken up to two times. **Option 2 –** To be costed with initial proposal. Additional training and support on how to achieve best working practices. This option may be taken up to three times. **Option 3 –** Not costed initially; a full cost will be requested before this option is taken. Technology refresh. **Option 4 –** Not costed initially; a full cost will be requested before this option is taken. Migrate the environment, or a specified portion of it (specified when the option is taken), to Redacted under FOIA Section 24 - National Security with appropriate mechanisms to allow updates and data transfer from the Redacted under FOIA Section 24 - National Security

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**
D – 1	*Progress reports*	*T0+1 Months*	*Presentation (.pptx), document (.docx), or alternative formal format proposed by supplier*	*n/a*	Redacted under FOIA Section 24 - National Securit	*Monthly until delivery of D-4 then quarterly* *Presentation pack to include but 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
D – 2	Initial specification and design	Supplier to propose Archimate preferred for architecture diagrams	Supplier to propose	n/a	Redacted under FOIA Section 24 - National Security	Required by the end of the discovery phase. This may be a confirmation, adjustments or update to the suppliers initial proposal and shall include design documentation and system architecture diagrams and artefacts.	DEFCON 705

D - 3	Redacted under FOIA Section 24 - National Security accredited environment at Early-Life Support (ELS) phase	T0+5 months	Software	8	Redacted under FOIA Section 24 - National Security	Supplier to propose detail of the how the environment will function at this milestone. At a minimum it must include: 1. Application and Developer user access from Dstl DONB, MODNET and a supplier acting as a developer/integrator 2. Each of the MVC applications working correctly on the environment with live sufficient DONB and Internet connectivity 3. Export (which may be a user managed process at this stage) to DONB or MODNET 4. Redacted under FOIA Section 24 - National Security	DEFCON 705
D – 4	Fully Operational Capability (FOC) environment	T0+9 months	Software	9	Redacted under FOIA Section 24 - National Security	An environment that meets all requirements in this SOR, fully tested, proven and accredited.	DEFCON 705
D – 5	Documentation and training	T0+12 months	Supplier to propose. Archimate preferred for	n/a	Redacted under FOIA Section 24 - National Security	Technical system documentation User documentation (an accessible electronic format is preferable)	DEFCON 705

			architecture diagrams			Provision of training to developers identified by the authority	
D – 6	MODcloud transition plan	T0+15 months latest	Word	n/a	Redacted under FOIA Section 24 - National Security	To include timeline, risks and outline technical activities. It is desirable that this is delivered as early as possible.	DEFCON 705
D – 7	MODcloud environment operational and accredited	T0+22 months	Software	9	Redacted under FOIA Section 24 - National Security	An environment that meets all requirements in this SOR functioning on MODcloud Updated documentation. It is desirable that this is delivered as early as possible.	DEFCON 705

***Technology Readiness Level required**

1.7	**Standard Deliverable Acceptance Criteria**
	As per G-Cloud terms and conditions. A period of 30 days shall be allowed for review of all deliverables by Dstl and provide comments to the supplier. 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. The technical detail shall be sufficient to permit independent reproduction of any process or system.
1.8	**Specific Deliverable Acceptance Criteria**
	Software, and Infrastructure as code, shall be sufficiently tested according to required quality, accreditation and MOD policy requirements by the supplier before delivery. Acceptance criteria these deliverables shall be articulated in the Statement of Work and agreed by the Authority. It may vary by deliverable as the maturity of the work evolves.

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**
	Compliance with MOD accreditation and security regulations, and other applicable policies.

3.	**Security**

3.1	**Highest security classification**	
	Of the work	Redacted under FOIA Section 24 - National Security
	Of the Deliverables/ Output	Redacted under FOIA Section 24 - National Security
3.2	**Security Aspects Letter (SAL)**	
	Redacted under FOIA Section 24 - National Security	
3.3	**Cyber Risk Level**	
	Redacted under FOIA Section 26 - Defence	
3.4	**Cyber Risk Assessment (RA) Reference**	
	Redacted under FOIA Section 26 - Defence If stated, this must be completed by the contractor 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://www.gov.uk/guidance/supplier-cyber-protection-service	

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	Redacted under FOIA Section 24 - National Security	Redacted under FOIA Section 24 - National Security	Contract award	Technical team	Disposal of copies not in environment

GFA-2	Redacted under FOIA Section 24 - National Security	Redacted under FOIA Section 24 - National Security	Contract award	Technical team	Disposal of copies not in environment
GFA-3	Redacted under FOIA Section 24 - National Security	Redacted under FOIA Section 24 - National Security	Contract award	Technical team	Disposal of copies not in environment

5. Proposal Evaluation criteria

5.1 Technical Evaluation Criteria

1. Does the proposal address the statement of requirement?
2. Do the deliverables correspond to those requested?
3. Is the proposal of sufficient technical quality to meet the requirement?
4. Are the resources and access to facilities aligned to the needs of the proposal, do they allow the measurements and necessary outcomes of the research to be met, including within the timescales proposed?

5.2 Commercial Evaluation Criteria

The supplier shall provide evidence to demonstrate that they can meet the following commercial requirements;

- A completed ‘Tasking Order Form’ confirming a resulting contract will be in accordance with the G-Cloud Terms and Conditions
- The supplier must provide their full FIRM price breakdown for all costs to be incurred to fulfil this requirement, including: any sub-contractor costs and the level of sub-contracting required, and any other costs applicable to this requirement.

The Authority will assess the proposal to ensure that all costs are fully detailed, and the price shall be commensurate with the work to be undertaken.

When placing any contract the Authority is required to satisfy itself that the agreed price represents Value for Money (VFM). In single source contracting you must provide to the Authority sufficient information in support of your price proposal and during subsequent price negotiation, to enable the Authority to fulfil its obligation to assure VFM. The Authority approaches all contract pricing on the basis of the NAPNOC principle (No Acceptable Price, No Contract). The Authority reserves the right to not enter into any contract that is unacceptably priced or unaffordable.