Serapis Tasking Form

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

To:	Lot 4 QinetiQ Plc	**From:**	Dstl

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

LOT 4 DSTL/AGR/SERAPIS/AII/01

VERSION CONTROL

Version 0.3

REQUIREMENT

Proposal Required by:	[31/08/2021]	**Task ID Number:**	AII71
The Authority Project Manager:	[REDACTED UNDER FOIA EXEMPTION]	**The Authority Technical Point of Contact:**	[REDACTED UNDER FOIA EXEMPTION]
Task Title:	ARA WP2.4 Improved Communications Situational Awareness		
Required Start Date:	[27/09/2021]	**Required End Date:**	[05/03/2022]
Requisition No:	1000167563	**Budget Range**	ROM Budget £150K (including Task Management Services)

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)

Background

This requirement is to explore and identify improved approaches to understanding openness modularity and flexibility in CIS Architectures. It is an activity within the Autonomous Resilient Architectures (ARA) project which seeks to develop and demonstrate self-discovering, self-connecting, self-coordinating architectures across a multi-domain, multi-classification, multi-national enterprises to provide improved C2, including in Denied, Degraded, intermittent and Low bandwidth (DDIL) environments.

We seek to complete this activity by March 2022 to inform our future plans for this project over the following three years.

The strategic framework document "Global Britain in a competitive age; The Integrated Review of Security, Defence, Development and Foreign Policy" outlines the following four overarching and mutually supporting objectives which includes:

1. *"Sustaining strategic advantage through science and technology: we will incorporate S&T (Science and Technology) as an integral element of our national security and international policy, fortifying the position of the UK as a global S&T and responsible cyber power.*
2. *Shaping the open international order of the future: we will use our convening power and work with partners to reinvigorate the international system.*
3. *Strengthening security and defence at home and overseas:*
4. *Building resilience at home and overseas: we will place greater emphasis on resilience"*.

A key S&T challenge is :

Multi-domain Command & Control, Communications and Computers (C4)–develop the capability for multi-domain integration and ability to coordinate effects globally enabling us to execute joint operations against adversaries with well-integrated and resilient capabilities.

Military Command & Control, Communications and Computers (C4)[1] is a broad, complex and technically challenging area characterised by rapid advances in technologies. The C4, is therefore, the connective tissue that provides the information needed to make decisions rapidly in a highly mobile, global and often infrastructure less environment.

Future C4 challenges

The future challenges in a C4 environment include the need for:

- new techniques and technologies that mitigate against rapidly emerging communications threats
- resilient and robust communications systems and architectures,
- connectivity to all mobile/static platforms (underwater, land, sea, air and space),
- global operations, often infrastructure less environment
- conducting operations that range from disaster relief, peacekeeping, surveillance to military engagement
- interoperability with national and international partners
- new architectures/protocols
- systems that are application aware
- satisfying convergence of systems and networks

To meet the challenges of Military C4, and address the Strategic Review aims, research needs to be conducted into Autonomous Resilient Architectures (ARA) with a key driver of demonstrating S&T technologies within the next 2 years.

The aim of the ARA programme is to exploit advances in S&T to develop self-discovering, self-connecting, self-coordinating architectures across a multi-domain, multi-classification, multi-national enterprises to provide improved C2, including in Denied, Degraded, Intermittent and Low bandwidth (DDIL) environments. To achieve this S&T activities may include:

- Research into Networks, Data & Information; to accelerate & bring together a variety of existing & emerging concepts & technologies. The aim would be to show how they can come together to deliver transformational architectural agility & flexibility. (This may include cross-stack agile resilience approaches)
- Contributing to future collaborations and demonstrations such as: FNC3; replacement to DIAS ITA initiative; other potential collaborations with a view to joint development & experimentation with international partners.
- S&T to strengthen our intelligent customer capability in this growing area by development of SQEP.

ARA Work Package 2 (WP2) (Adaptable Communication Services (ACS)) will accelerate research into the adaptation of deployed/tactical Communications and Information Systems (CIS) to meet changing operational goals and associated deployment environment. Service adaptations within scope of this work package include:

- Agile infrastructure that can change posture in line with mission goals, for example, by changing traffic prioritisations and/or which underlying bearers are used;
- Adaptation of application behaviours to suit current radio conditions, for example, by changing codec, adjusting image quality or changing between reactive and proactive content distribution paradigms.

[1] Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors

A key enabler for this adaptation is the definition of policy that defines the mission goals, and what actions different components of the communications services are permitted to take in response to events that impact availability of resources.

Underpinning this adaptation of infrastructure resources is improved network Situational Awareness (SA), both for the administrative users tasked with monitoring and maintaining the infrastructure, and for any future automated network management functions.

Aim

The aim of this SoR is to assess current commercial approaches to monitoring network infrastructure in order to improve network SA and develop recommendations for how these solutions can be exploited in military CIS, to enable ACS. A key requirement of the solution will be to have a unified approach to monitoring disparate underlying communications systems.

This Task is intended to cover the full-breadth of MOD network management solutions, across Land, Sea, Air and Joint domains.

Requirement

Requirement #1: Survey and Evaluation of Network Monitoring Solutions for ACS

A survey of the state-of-the-art in commercially supported network monitoring solutions is required to characterise different architectural approaches that could be used to support improved Network SA. This should incorporate specialised solutions tailored to highly dynamic and flexible environments (such as tactical radio networks) as well as Enterprise systems that nonetheless can scale-down to efficiently support the DDIL environment. It is desired that the range of solutions cover a breadth of approaches (e.g. to avoid ending up with all solutions being similar and based around one or two common technologies e.g. SNMP – unless that is all that exists.)

The surveyed solutions should include those used in extant MOD deployed systems such as Skynet 5 and Falcon (from Land, Sea, Air and Joint (represented by the Global Operations and Security Control Centre (GOSCC)) and including the Service Management Integrated Technical Solutions (SMITS) capability), capturing, at a high level, the main features of any bespoke systems that differentiate them from commercial offerings, especially around agility and flexibility. It is not expected that the current network management systems will be fully documented in this task. There is particular interest in information like e.g. what military specific features do the bespoke solutions offer?; what can’t those solutions do that would be desirable?

Finally, a view of future trends in network monitoring technology is required, including from standards organisations and academic research. Of particular interest are systems designed to make use of Machine to Machine (M2M) interfaces that could be driven by Artificial Intelligence (AI), automatically enacting policies appropriate to the environment. In addition, the capability to allow Third Parties (e.g. App developers) to efficiently extend these systems is also of interest. Ideally, the systems will provide an Application Programming Interface (API) to access their internals, potentially with a pre-existing ecosystem (cf. App store) already in place. Examples of novel/interesting Third Party extensions should be described, with potential linkages to the military domain.

The information captured for each solution must enable their categorisation and an evaluation of strengths and weaknesses to take place. It is desired that fundamentally similar approaches based on common technologies should be aggregated together in this assessment. The criteria required (to drive the information capture) is to be defined by the Task, but should include (at a minimum):

- Broad technical approach
- Solution name, company and ownership (or examples thereof);
- Technical description, category (e.g. Enterprise, Tactical), availability (Open Source, Commercial, Bespoke), protocols supported, e.g. NETCONF, SNMP etc., adaptability/extensibility and existing Third Party ecosystem;
- Suitability to, and flexibility of use in DDIL environments (e.g. in terms of resilience, robustness, overheads (network and compute), dependencies etc.);

It is expected that this work could also be exploited by Army HQ’s IR2E (formerly JimmyWorks).

Requirement #2: Study of Network Monitoring Information and Its Usage for ACS

A study of the information that can be derived from a network monitoring solution is required, as well as the information needed to support key network management actions. This should identify broad categories of information, e.g. router packet statistics, rather than specific configuration items. A bounded number of worked examples are then required to demonstrate how a subset of these information categories could be used by an intelligent system (e.g. Human, expert AI) to inform beneficial changes in the CIS posture. For example, use of Quality of Service (QoS) metrics to dynamically engineer alternative routes across a network. These should be innovative in nature and not simply re-stating existing technologies such as Multiprotocol Labelling Switching (MPLS). The examples should be aimed at the DDIL environment.

Requirement #3: Study of Network Monitoring Architectures

An architecture study is required to consider how the solutions identified in the survey can be applied to the MOD system of systems network architecture. This study should propose options to identify how multiple, extant, disparate monitoring solutions could be unified under a new approach. This could include a future migration to a core solution that allows sub-systems to be bolted-in through well-established interfaces, protocols or standards. As part of this study, solution architectures should identify options and techniques for integrating and managing the security constraints of different systems. Awareness of traditional commercial and contracting barriers to any proposed solutions should be stated.

It is desired that this work seeks to avoid straying into the cross domain security solution space, as it is not the main emphasis of this study (but may be explored more in future). This requirement is looking at potential areas of the architecture where such solutions may be needed for information sharing, but not looking for specific cross domain solutions at this point in time.

Outcomes

Recommendations are required to inform future deployed network monitoring approaches. These should include:

- Commercially supported solutions that are cognisant of the DDIL environment, while offering scope for agility and extensibility and future AI-driven interfaces to enable ACS;
- How network management information can be used to guide and drive changes to network that could benefit the military CIS posture;
- Network management architectures that offer a unified approach to monitoring disparate underlying communications systems.

Innovation Benefits and Exploitation Plan (IBEP)

By conducting the work the following are anticipated.

1. Innovation – (i.e. what are we building on?)
    a. Network management know-how in a military/civil domain;
    b. Previous architectures for system of systems solutions;
    c. Previous commercial collaborations;
    d. Application of AI and novel configuration management to the DDIL environment;

2. Benefits (i.e. what will the contracted academic stakeholders get from this?)
    a. Novel application of developing technologies for Defence;
    b. Access to industrial Defence sector expertise;
    c. Development of new capabilities;
    d. Closer Defence-sector / commercial collaboration;

3. Exploitation (what are the artefacts that Dstl will get that can be more widely exploited)
    a. Army HQ 6Works (formerly JimmyWorks);
    b. Know-how in the Defence Industrial base (papers, reports, presentations);
    c. Know-how in the Academic supply base;
    d. Potential new recruits into the Defence supply chain if UK resources used;
    e. Testing of proposed architectures through the ISS Design Pillar;

4. Plan (what's the plan for exploitation)
    a. Input into the wider WP2 ACS initiative;
    b. Potential for accelerating know-how (facilities, hardware, configuration) through Industrial exploitation;
    c. Briefings to MOD Stakeholders;

Outputs

Outputs (or artefacts) of the Task activities that may be exploited more widely could include:

- Literature survey of commercially supported network management solutions;
- Architectural designs and analysis for system of systems network management solutions;
- Recommendations for build and integration of network management solutions into a future project testbed?

Deliverables

The formal deliverables (progress reports and presentations) of the project are highlighted in the Deliverables section.

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	TRL	Expected classification (subject to change)	Information required in deliverable	IPR DEFCON
D-1	Monthly progress reports (MPR)	T0+1 month	Presentation		[REDACTED UNDER FOIA EXEMPTION]	PORT (progress, opportunities, Risks, Timelines) quad chart presentation pack	703
D-2	Fortnightly Progress and Technical Review	Every 2 weeks	Meeting Minutes by Email		[REDACTED UNDER FOIA EXEMPTION]	Agenda to include but not limited to: • Update on technical progress • Progress report against project schedule • Review of deliverables • Risks/issues • GFA and supplier performance	703
D-3	Final Report	T0+4 months	Report (Word)		[REDACTED UNDER FOIA EXEMPTION]	Report to include: • Aims • Technical Progress • Achievements • Exploitable outputs • Recommendations	703
D-4	Final Presentation	T0+4 months	Presentation (Powerpoint)		[REDACTED UNDER FOIA EXEMPTION]	• Presentation of the Final Report	703

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)*

Unique Identifier/ Serial No	Description	Classification	Type	Available Date	Issued by	Return or Disposal Date	Any restrictions?

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

[REDACTED UNDER FOIA EXEMPTION]

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

Cyber Risk Level	[REDACTED UNDER FOIA EXEMPTION]
Risk Assessment Reference	[REDACTED UNDER FOIA EXEMPTION]

ADDITIONAL TERMS AND CONDITIONS APPLICABLE TO THIS CONTRACT

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 **QINETIQ/21/04536** **(attached)**

The proposal includes:

- A full technical proposal that addresses the individual activities that are detailed in Statement of Requirements (Part 1 to Tasking Form).
- A work breakdown structure/project plan with key dates and Deliverables identified including required delivery dates for Government Furnished Assets.
- A clear identification of Dependencies, Assumptions, Risks and Exclusions which underpin your Technical Proposal.

A breakdown of deliverables and Interim Payments (Milestone/stage) due dates is provided below.

Sub-Contractors personnel particulars Research Worker Form and security clearances (if applicable)

COMMERCIAL

As per the Serapis Limitation of Liability Discussion Paper Agreement, this task will fall under the band of a cap on liabilities of £500,000.

No Background IP

PRICE BREAKDOWN

A Firm Price Quotation of ***£149,561.29*** *(one hundred and forty nine thousand, five hundred and sixty one pounds, twenty nine pence) (ex VAT) is submitted for the Task AII52 and broken down as shown in the tables below.*

It should be noted that the following effort associated with this task will be charged against AII102 DCEAT/ARA Management and Enablers:

- Associate Technical Partner support.

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

Total Proposal Price in £	£149,561.29		(ex VAT)
Start Date:	January 2022	**End Date:**	April 2022
Lot Leads Representative	Name	[REDACTED UNDER FOIA EXEMPTION]	
	Tel	[REDACTED UNDER FOIA EXEMPTION]	
	Email	[REDACTED UNDER FOIA EXEMPTION]	
	Date	26th January 2022	
Position in Company	Assistant Commercial Manager		
Signature	[REDACTED UNDER FOIA EXEMPTION]		

Core Work – Breakdown

[PRICING TABLES REDACTED IN ENTIRETY UNDER FOIA EXEMPTION]

[PRICING TABLES REDACTED IN ENTIRETY UNDER FOIA EXEMPTION]

Core Work – Milestone breakdown costs
Proposed Milestones Payments

[PRICING TABLES REDACTED IN ENTIRETY UNDER FOIA EXEMPTION]

[PRICING TABLES REDACTED IN ENTIRETY UNDER FOIA EXEMPTION]

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	26/01/2022
Requisition Number		1000167563
Contractor's Proposal Number		AII71 ARA WP2.4 Improved Communications Situational Awareness
Purchase Order Number		TBC
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.		