Serapis Tasking Form

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

To:	Lot 4 QinetiQ Plc	**From:**	The Authority
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 0.1			
REQUIREMENT			
Proposal Required by:	15/10/2021	**Task ID Number:**	AII69
The Authority Project Manager:	[REDACTED]	**The Authority Technical Point of Contact:**	[REDACTED]
Task Title:	Military Systems Information Assurance: DCS, GVA, ZTA.		
Required Start Date:	31/10/2021	**Required End Date:**	31/03/2022
Requisition No:	[REDACTED]	**Budget Range**	WP1: 500k WP2: 500k WP3: 800k (Costs inc Serapis Mgmt Charges)
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)

Overall Scope of this SOR:

This tasking form details the requirements for a set of 3 associated pieces of work that will be undertaken for the Military Systems Information Assurance Project. These tasks are:

WP1 IBSA Development (IBSA)
WP2 Integration of DCS and the Generic Vehicle Architecure (GVA)
WP3 Zero Trust Development Environment (ZT)

The Statement of Requirements is split into 3 sections, each addressing one of the above.

All work will be carried out under DEFCON 703 unless specified (see IBSA-R4 and GVA-1)

WP1- IBSA Development (IBSA)

IBSA-Background:

Data Centric Security (DCS) is an emergent security approach that emphasises the importance of protecting data rather than networks to gain information advantage.

To date, Dstl research into Information Based Security Approach (IBSA) has been carried under the Single Information Environment Interoperability (SiEi) IBSA Research Project and this has delivered an IBSA Architecture, IBSA Test System and international interoperability trials with other NATO DCS systems and corss-domian guards, up to Technology Readiness Level (TRL) 6.

UK STRATCOM are currently leading UK activities to exploit outputs from the SiEi IBSA Research Project from TRL6 upwards, through an series of Interoperability demonstrations and excersises with US CENTCOM.

This SOR will complement the above UK STRATCOM work through research into the expansion and consolidation of the outputs of the SIEi IBSA Research Project, to accelerate and enhance the use of DCS in MOD systems, through the demonstration of Generation after next capabilities into both Enterprise and Tactical systems. This work should be up to TRL6.

[REDACTED]

This SOR should deliver in FY21/22.

IBSA- Requirements:

IBSA-R1: Metadata Schemas: Creation of a family of DCS Metadata schemas that provide the ability to scale DCS rom Tactical to Enterprise levels, with the appropriate Fields to support UK Sovereign requirements. This should seek to provide a UK Soverign schema, but must maintain compatibility with both TDF and current NATO strandards/policy. The primary driver for this is Interoperabiltiy with the US and NATO. The schemas should encompass both XML, to be compatible with exsiting national and NATO requirements, and machine readable implementations.

This should consider the whole life cycle of the data (ie from creation through to archiving).

The deliverable will be:

A report detailing the Metadata schemas required and the associated schema management tooling (as an example TDF can use Schematron).

IBSA-R2: Cross Domain Approaches: DCS brings fresh challenges as well as fresh opportunities and the current approach and policy towards secure Cross Domain information transfer may not be appropriate in Architectures that incorporate DCS technologies.

This task will be an investigation into how the Cross Domain Security enforcement functionality would be implemented in using DCS technologies, and how this functionality would be delivered in a mixture of a DCS and network centric environments.

This work should address MOD Cross Domain Policy as governed by JSP 604 (specifically Section 5), but this should be used as a starting point and any finidngs should identify where current policy should be challenged if a better outcome can be delivered in a manner that is not compliant with current Policy

The output will be a report with recommendations as to how Cross Domain Security enforcement functionality would be implemented in a DCS environment (this should include the interface between DCS and non-DCS systems).

IBSA-R3: IBSA DCS Format(s) Expansion: In order to extend DCS research IBSA need to support additional data formats. This task is to implementation JCHAT, Streaming Video data formats and email into the current IBSA baselined system.

In this instance DCS email is defined as being where the body of the email is a DCS object (as opposed to a standard email solution that delivers a DCS object as an attachment).

Deliverables from this Requirement will be a report on how JCHAT and Streaming Video data formats, and DCS email can be implemented into IBSA, together with a costed option for integration into the IBSA system.

IBSA-R4: DCS Black LAN enablement. This task will look at how physical and Information security can be maintained in a DCS environment and will address two areas:

- How can local print services be implemented in a DCS environment.
- How can a DCS Encryption/Decryption capability be provided at a DCS End Point (ie user access device)

DEFCON 705 will be considered for this Requirement if it involves previous IP from the supplier. This should be documented in the Proposal.

Deliverables from this Requirement will be a report on how DCS Black LAN enablement can be achieved in IBSA together with a costed option for a demonstrator showing the above requirements. The DCS engine for any demonstrator must be based on the current IBSA test instantiation.

IBSA-R5: SME Support to Dstl. This task is to provide 30 days ad hoc SME call off to progress DCS work from contract start to end of FY20/21. This includes DCS SME support for Autumn TIDESprint and crypto support for Dstl engagement with BATCIS for review of Crypto Architectures.

WP2 - Integration into the Generic Vehicle Architecure (GVA)

GVA-Summary

The overall MSIA project will deliver a “Systems of Systems demonstration of ability to scale Data Centric Security (DCS) technologies to representative user network” in FY24/25 This work will form the first part of this work, and will

To carry out a series of activities to investigate, test and integrate a Data Centric Security (DCS) approach into the Land Generic Vehicle Architecture (GVA). The objective include:

- Identifing potential options for the integration of DCS and GVA
- Implementing and testing selected option(s) from the above
- Integrating into an existing DCS architecture to demonstrate integration of GVA with a wider information environment,
- Briefing the above to MOD Stakeholders.

GVA-Background Information

Dstl have been working for a number of years on a concept known as Data Centric Security (DCS), the underpinning aspects of which are the creation of metadata[1], encryption of that metadata and data with cryptographic binding of the two elements to create a single DCS Object.

To full enable, deliver and exploit a future Single Information Environment whilst realizing Information Advantage, DCS is seen as a key enabler in the approach to being able to deliver (push) or access (pull) Information at the point of need.

The concept of DCS has been developed to a high level of maturity and is currently being investigated by UK STRATCOM with a view of deploying a DCS at the enterprise level in the near future. Dstl (as the UK lead in DCS) has also been working with other NATO Partners, looking at DCS interoperability and the development of a number of DCS Standards & Definitions.

As part of this work NATO has defined three levels of DCS[2] (Ref A below):

- DCS Level 1 (L1) – Basic Labelling: binding and verifying confidentiality labels (no cryptographic mechanisms)
- DCS Level 2 (L2) – Enhanced Labelling: data and metaData are cryptographically bound but are not encrypted.
- DCS Level 3 (L3) – DCS Object Cryptographic protection: Data and MetaData are cryptographically bound. Data and MetaData are encrypted.

Whilst the current Dstl Candidate implementation of DCS can consume and generate NATO compliant DCS Objects inline with Ref B and C, it uses the Trusted Data Format Ref [d] natively.

To date, DCS research has focussed to date on Enterprise level systems and now that the approach has matured and been tested both nationally and internationally it has been decided that now is a suitable juncture to

commence investigation into the integration and deployment of DCS into the more challenging operational areas of defence and to further the concept of a wider Single Information Environment.

This work will be the initial steps into implementing DCS in more challegning Tactical envirments. Initial proposals will be developed to integrate DCS within Platform architectures and this will be demonstrated in a GVA Concept Demonstrator. This will demonstrate how DCS can be scaled within Systems of Systems (ie between Operation and Tactical CIS).

The GVA has been chosen because many Land Vehicles have to be able to support multiple systems and services that run at different classifications within the platform. DCS provides a mechanism for enabling the the logical separation of data at differing Classifications which has a potential benefit of reducing the underlying physical infrastructure to a single network.

[1] A collection data objects that describes the properties of some related data, typically associated with a metadata schema, which is a logical model that shows the relationships between metadata elements.

[2] An information object that is formed of the following components; a data element, metadata related to the data element which contains other metadata conformant with the metadata schema being used (4774/8 or TDF), and a binding element that binds the two elements together.

The current version of GVA uses the Data Distribution Service (DDS) protocol to transfer information within the vehicle platform. An extension to DDS, (called Secure DDS) has been developed by third parties which may be of potential use.

The initial activity (R.1) is to investigate how best to integrate DCS with GVA and the underlying protocol DDS and/or Secure DDS.

As this work will entail the integration of Crown Owned IP, elements of this work that pertain to the integration of DCS into GVA are to be carried out under DefCon 703 to retain the Crown Owned IP. The output should be DEFCON 703 unless commercial IP is proposed by a supplier. In this instance DEFON 705 can be used for exisiting commercial IP and this must be documented in the Proposal.

GVA-Requirements

The requirements for this SOR are to carry out:

GVA-R1: A study into the optimal mechanism for integration of Data Centric Security and the GVA and the underlying DDS protocol. The deliverable from GVA-R1 will be a report as to how DCS and the GVA should be integrated together with a costed option to deliver the following:

- A concept demonstrator that shows the integration of DCS and the GVA. This must show interoperability between a Brigade HQ and a vehicle, and between two vehicles.
- Evaluation and Report on implementations (import, export, within harness data flows)
- The above evaluation must include testing of data transfer (import, export and data transfer across the test environment) with a Report containing results of all tests, findings and recommendations for future options.
- Stakeholder Demonstration(s), to include the production of Briefing materials
- It is envisaged that at this stage the work will be classified at Official and that all work can be carried out in the existing IBSA UK Cloud environment (or similar).

GVA-Timelines

GVA-R1 to be produced by end of FY21/22.

The concept demonstrator must be ready by end of FY22/23

WP3 - Zero Trust Development Environment (ZT)

ZT-Background Information

An emerging cyber resilience requirement is the Zero Trust Architecture (ZTA) security model for critical networks. For cyber defence of MOD system(s), arguably the **most** critical component within the lifecycle of a system is the development toolchain.

For any system, the greatest cyber risk is that of the adversary compromising the development toolchain[3], and in a system that is viewed as 'critical' the requirement to secure that development toolchain and the environment that surrounds it becomes ever more important.

Compromising the development environment is the holy-grail for Cyber attackers, a most recent example of this is Solarwinds which has been described as equivalent to a Pearl Harbour attack. Compromising the development tool chain enables the adversary a route to freedom of action and manoeuvre for cyberattack. A compromised system development toolchain enables the adversary to create a tailored exploitation for that system.

Securing the system development toolchain and its environment is a significant challenge, particularly for complex projects where the system is incrementally developed and spread over many networks, physical sites and organisations. For example, the global development chain for F35 consists of more than 1900 companies spread over more than 10 countries.

Dstl have been working for a number of years on a concept known as Data Centric Security (DCS), through the Information Based Securty Approach Project (IBSA). The underpinning aspects of DCS are the creation of metadata, encryption of that metadata and data with cryptographic binding of the two elements to create a single DCS Object.

The concept of DCS has been developed to a high level of maturity and is currently being investigated by UK STRATCOM with a view of deploying a DCS at the enterprise level in the near future. Dstl (as the UK lead in DCS through IBSA) has also been working with other NATO Partners, looking at DCS interoperability and the development of a number of DCS Standards & Definitions.

As described above, the ability to protect systems **even during development,** is seen as a requirement to counter the possibility of an adversary compromising development environments. It has been identified that the combination of a ZTA when combined with DCS has the potential to deliver a resilient and secure development environment that spans the UK Defence supply chain.

ZT-Summary of Long Term Research

To research, develop and demonstrate through experimentation, a first in class Zero Trust Development Environment (ZeTruDE). This task should include an evaluation into whether a combination of approaches such as Zero Trust Architecture (ZTA), Data Centric Security (DCS) Architecture, or other approaches, can achieve the objectives of ZeTruDE. This should consider:

a. Scaling to the size and complexity of a project that is supported by global development chain (F35, for example, consists of more than 1900 companies spread over more than 10 countries)
b. Demonstrating the ZTA 'never trust and verify' principle for every development artefact for every system software build
c. Protecting individually every development artefact whilst at rest
d. Controlling individually access to every development artefact
e. Generating and maintaining a non-reputational provenance record for every development artefact and output artefact
f. Assisting the ZTA in assuming a breach principle by enabling the rapid traceability of the provenance of every change in every development artefact with non-repudiation
g. Implementing a version control system for all artefacts.

The system is to follow Open Architecture principles and be modular in design with documented interfaces, and a document API, to allow for future expansion.

The final output of this work will be a TRL6 ZeTruDE Architecture and Candidate (Minimal Viable) System.

ZT- Requirements

[3] Software Libraries, include files, models, compiler

This SOR is the initial stage towards delivering a ZeTruDE development environment with the final output of this phase being a Costed Option for a ZeTruDE Concept Demonstrator.

ZT-R1: ZeTrude Use Cases and Prioritised Requirements

Define and prioritise requirements for a ZeTruDE through a set of Stakeholder workshops to identify and define Use-Cases that represent MOD product development cyles with respect to Software. A list of initial high-level requirements is given below and it is expected that the list of requirements generated from the workshops will contain a more complete set.

a. Scale to the size and complexity of a complex project that is supported by global development chain (F35, for example, consists of more than 1900 companies spread over more than 10 countries)
b. Demonstrate the ZTA 'never trust and verify' principle for every development artefact for every system software build
c. Protect individually every development artefact whilst at rest
d. Control access to every development artefact individually
e. Generate and maintain a non-repudiational provenance record for every development artefact and output artefact
f. Assist the ZTA in assuming a breach principle by enabling the rapid traceability of the provenance of every change in every development artefact with non-repudiation
g. Have a version control system for all artefacts to meet the above requirements.

The deliverable for ZT-R.1 will be a report containing the Use-Cases and prioritised requirements for the ZeTruDE.

ZT-R2: Provenance

Research and develop provenance technology (such as distributed ledger technology) that will work within a ZeTruDE to enable full traceability to all changes in all development artefacts for the system/software development toolchain.

The deliverable for R.2 will be a report documenting how the the full provenance traceability requirement will be met within the ZeTruDE and how it will be implemented.

ZT-R3: ZeTrude Architecture

Develop and document ZeTrude Architecture that will support the capabilities given in R1 and those further identified in the deliverables from R1 and R2.

If a DCS element is included, this must be based on the outputs of previous Dstl Information Based Security Approach (IBSA) research.

The deliverable from ZT-R3 will be a report that documents the proposed architecture.

ZT-R4: Costed Options to build a Concept Demonstrator which will be used for the following purposes:

- Conduct scaled experiments that demonstrate the utility and practicality of a ZeTruDE
- Conduct red-team scaled experiments the ZeTruDE to find shortfalls and limitations
- Demonstrate the ZeTruDE with a project that is a real development (PYRAMID/Tikal/CESTIUS) or a provided legacy development (Tornado legacy toolsets).

The deliverable for R.4 will be a a costed option proposal.

ZT - Timescales:

The expected timescales for this SOR are:

Nov 21: Workshops for R1

Jan 21: Deliver R2

Apr 21 (ie end of FY21/22): Deliver R3 and R4

FY22/23 Take up of costed option from R4.

References:

A. NATO DCS Strategy and Vision Paper

B. NATO STANAG 4774 Metadata labelling for Confidentiality

C. NATO STANAG 4778 Binding Profiles

D. Trusted Data Format (TDF)

E. DDS (https://www.dds-foundation.org/)

Definitions

Metadata: A collection data objects that describes the properties of some related data.

Metadata Schema: A logical model that shows the relationships between metadata elements.

Cryptographic Binding: Associating two or more related elements of information using cryptographic techniques.

DCS Object: An information object that is formed of the following components; a data element. Metadata related to the data element and contains other metadata conformant with the Metadata Schema being used (4774/8 or TDF), and a binding element that binds the two elements together.

Transfer of DCS Objects: The transfer of DCS Objects between two DCS systems over a specified network, where System A and System B are either side of the Network, such that a User on System A can search the object store of System B and retrieve a DCS Object. The user should then be able to edit and save the encapsulated document, which is then sent as a DCS Object back to original object store on System B. The file must travel across the network at the specified DCS Level (see below) at all times (eg for Secure Transfer of Level 3 DCS Objects the DCS object must travel across the network at DCS Level 3 at all times).

DCS Levels:

- DCS Level 1 (L1) – Basic Labelling: Binding and verifying confidentiality labels (no cryptographic mechanisms)
- DCS Level 2 (L2) – Enhanced Labelling: Data and MetaData are cryptographically bound. Data and MetaData and not encrypted.
- DCS Level 3 (L3) – DCS Object Cryptographic protection: Data and MetaData are cryptographically bound. Data and MetaData are encrypted.

Single Information Environment: An information environment whereby information can be accessed by a user at the point of need, wherever that user is logged on.

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 [REDACTED] 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 AND OUTPUTS

[REDACTED]

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

- Access to IBSA Cloud-Based Test System
- Access to Dstl IBSA Candidate System Pre-Production
- Access to IBSA code base and associated documentation

- Dstl to attend Task related events.

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

The highest classification of this SOR
OFFICIAL □ OFFICIAL-SENSITIVE □ SECRET □ TOP SECRET □ STRAP □ SAP □

The highest expected classification of the work carried out by the contractor
OFFICIAL □ OFFICIAL-SENSITIVE □ SECRET □ TOP SECRET □ STRAP □ SAP □

The highest expected classification of Deliverables/Output
OFFICIAL □ OFFICIAL-SENSITIVE □ SECRET □ TOP SECRET □ STRAP □ SAP □

Note: It is expected that some apsects of WP5-GVA will at Official-Sensitive. All other work will be Official.

Is a Security Aspects Letter (SAL) required? *(A Security Aspects Letter (SAL) will be required for each Task above Official-Sensitive and above)*

Yes □ No □

TASK CYBER RISK ASSESSMENT. *[REDACTED]*

Cyber Risk Level	[REDACTED]
Risk Assessment Reference	[REDACTED]

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 **[REDACTED]** **(attached)**

Delivery of the requirement:

The proposal shall include, but not be limited to:

- A full technical proposal that meets the individual activities that are detailed in Statement of Requirements (Part 1 to Tasking Form).
- Breakdown of individual Deliverables, with corresponding Intellectual Property rights applied.
- Breakdown of Interim Milestone Payments, with corresponding due dates.
- A work breakdown structure/project plan with key dates and deliverables identified.
- A list of required Government Furnished Assets from the Authority, including required delivery dates.
- A clear identification of Dependencies, Assumptions, Risks and Exclusions which underpin your Technical Proposal.
- Sub-Contractors Personnel Particulars Research Worker Form and security clearances (if applicable)

COMMERCIAL

[REDACTED]

PRICE BREAKDOWN

You are to use the costs detailed in Item 2 Table I in the Schedule of Requirement and at Annex E Table 2 of the Serapis Framework Agreement. Please also provide a price breakdown which should include, but is not limited to: Lot Lead Rates, Sub-contractors costs and rates, travel and subsistence. In support of your Proposal you are requested to provide clear details of all Dependencies, Assumptions, Risks and Exclusions that underpin your price.

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

Total Proposal Price in £	£1,786,887.02		(ex VAT)
Start Date:	10/1/22 (tba)	**End Date:**	31/3/22 (tba)
Lot Leads Representative	Name	[REDACTED]	
	Tel	[REDACTED]	
	Email	[REDACTED]	
	Date	[REDACTED]	
Position in Company	[REDACTED]		
Signature	[REDACTED]		

Core Work – Breakdown

[REDACTED]

Core Work – Milestone breakdown costs

Proposed Milestones Payments

Your TMS bid costs shall be included in milestone 1.

The final Milestone must reflect the actual cost of the deliverable, and be greater than 20% of the Task value, unless otherwise agreed with your Commercial POC

Please duplicate the template per milestone table format below as necessary, and rename milestone number accordingly.

[REDACTED]

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]
	Tel	[REDACTED]
	Email	[REDACTED]
	Date	[REDACTED]
Requisition Number		[REDACTED]
Contractor's Proposal Number		[REDACTED]
Purchase Order Number		[REDACTED]
Signature		[REDACTED]
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.		