Statement of Requirement (SoR)

Reference Number	RQ0000002570
Version Number	**1**
Date	**17/01/2022**

1.	**Requirement**
1.1	**Title**
	UK AR&AS IT Health Check
1.2	**Summary**
	An IT Health check on the UK Acoustic Replay &Analysis (UK AR&AS) system in Dstl Underwater Group (UWG), according to the scoping meeting. This would be preferable to start post April 2022 and the deliverable is a report back to UWG.
1.3	**Background**
	[redacted]We are required to go to Crown Commercial Services who source contractors assured by the National Cyber Security Centre (NCSC) with our IT Health Check requirement.
1.4	**Requirement**
	The ITHC shall comprise the following main activities: a. Scoping Meeting (approx. 1 month prior to test) - Delivery of an agreed work plan b. Conduct of Test (including but not limited to) • Network scan of all devices. • Scan all servers and a selection of workstations for up to date patches. • Check select applications for vulnerabilities.

	• Check representative workstation for lockdown. • Show any exploits found, consult UWG before exploiting due to work happening on the system. • Provide a report on completion detailing vulnerabilities and recommendations. • Provide an [redacted] executive summary. These are the general mandatory requirements – specifics usually discussed at the scoping meeting. c. Post Test review Meeting d. Final Report Approach The scoping meeting is usually around a month before testing begins and should allow time for further preparation. The scoping team should comprise; a representative from an assured NCSC provider, and from Dstl, the Secure Systems Network Manager, MOD / Dstl accreditor, IT Security Officer and the Facility Manager. Work will be monitored on whether the areas defined in the scoping meeting have been tested to the degree agreed. NCSC approved staff requirements will be discussed at the scoping meeting but previously 2 testers have spent 5 days on-site testing the system and writing up results. The staff are required to have a DV clearance. The staff are required to be assured by NCSC so will meet NCSC's (skills and other) criteria for this work.
1.5	**Options or follow on work**
	Not Applicable

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**
D1	Report detailing findings of tests. Detail and format to be agreed at scoping meeting.	ASAP starting 2022 FY.	Electronic report.	N/A	[redacted]	Report findings of IT Health Check with recommendations. An executive summary at a lower classification is required.	Cyber Security Services 3 DSP terms apply
D2	Agreed work plan	4 weeks before agreed ITHC date	Electronic report		[redacted]	Summary report of the scoping meeting	Cyber Security Services 3 DSP terms apply

*__Technology Readiness Level required__

1.7	**Standard Deliverable Acceptance Criteria**
	All reports included as deliverables under the contract must comply with the Defence Research Reports Specification (DRRS), which defines the requirements for the presentation, format and production of scientific and technical reports prepared for MoD. All deliverables shall be supplied in accordance with the Security Aspects Letter for this task. All deliverable documents and reports shall be provided in Microsoft Word 2016; all Gantt charts in Microsoft Project 2016 format and all presentations in Microsoft PowerPoint 2016 format.
1.8	**Specific Deliverable Acceptance Criteria**
	An executive summary at a lower classification is required.

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:** NCSC Approved (Please specify below)
2.2	**Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement**

3.	Security	
3.1	**Highest security classification**	
	Of the work	[redacted]
	Of the Deliverables/ Output	[redacted]
3.2	**Security Aspects Letter (SAL)**	
	Yes If yes, please see SAL reference- RQ0000002570	
3.3	**Cyber Risk Level**	
	[redacted]	
3.4	**Cyber Risk Assessment (RA) Reference**	
	Risk Assessment Ref: [redacted] 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://suppliercyberprotection.service.xgov.uk/ . Please Note: The previous Cyber Risk Assessment portal has been closed down. There is currently an interim process in place for three months until September 2021 while a new portal is being created. Follow the process below for this ITT. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow, if a RAR reference is stated above, a SAQ Form must be completed by the contractor before a contract can be awarded. A PDF version of the form has been included as part of the ITT for this purpose. Please complete the form and return it to ISSDes-DCPP@modnet.r.mil.uk during the tender period. A SAQ reference will be generated	

	and sent in response within a few days. The SAQ reference must be included with the tender response. A Cyber Implementation Plan (CIP) should also be included if appropriate. Flow down to Sub-contractors

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+)
GFE-1	SNx	Workstation	During Contract	UWG	End of Contract
GFE-2	SNx	Workstation	During Contract	UWG	End of Contract
GFF-1	N/A	Desks, chairs.	During Contract	UWG	End of Contract

5.	Proposal Evaluation criteria
5.1	**Technical Evaluation Criteria**

Technical Criteria 60%

Proposals will be assessed by the Dstl Project Technical Authority and Commercial Authority using the following criteria and weighting.

This requirement will be competed and awarded on the basis of best Weighted Value for Money Index. The winning tender will be subject to available funding. DSTL reserves the right to fail a tender exceeding the unrevealed limit on grounds of unaffordability.

Technical criteria 60%

Cost 40%

Tenders will be technically evaluated using the criteria supplied in the following table. The maximum technical score is 30, the minimum score is 0.

Descriptions of the criteria and what constitutes an excellent to poor response are provided. A score of 0 or 1 in any of the criteria will result in the tender being assessed as technically non-compliant and will be excluded from the competition.

The three technical criteria are equally weighted.

Technical Category	Max Score (0-10)
Describe how would you ensure that vulnerability assessments are carried out to an acceptable standard without affecting a live environment?	10
Describe how your final report will meet the objectives of the requirement (e.g. structure, length, audience, etc.).	10
How do you structure your approach whilst penetrating a network in a layered environment?	10

Mark	Criteria

	0 – Unacceptable or no answer	Has demonstrated inadequate experience or provided inadequate supporting evidence which gives no confidence of the Potential Tenderer's competence and an unacceptably high level of risk to the project
	1 – Poor response with Very High risk	Has demonstrated narrow experience or provided minimal supporting evidence which gives low confidence of the Potential Tenderer's competence and a very high level of risk to the project.
	4 – Satisfactory with Medium to High risk	Has demonstrated some experience and provided adequate supporting evidence which gives some confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.
	7 – Good with Low to Medium risk	Has demonstrated broad experience and provided adequate supporting evidence which gives confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.
	10 – Excellent with Very Low risk	Has demonstrated considerable and detailed experience and provided sound and relevant supporting evidence which gives high confidence of the Potential Tenderer's competence and a very low level of risk to the project.
5.2	**Commercial Evaluation Criteria**	

Element	Requirement	Weighting
C1	Compliance with the Cyber Security Services 3 terms and conditions	Pass/Fail
C2	Please submit your full firm price breakdown for all costs to be incurred, including: • Labour costs • Travel & Subsistence costs • Any Materials costs • Any Facility costs • Any Sub-Contractor costs • Any other costs	Pass/Fail

Mark	Definition
Pass	Fully meets the Authority's requirement. Provision and acceptance of the sub-criteria information in the format requested, which is clear, unambiguous and transparent.
Fail	Unacceptable/Nil Return. Tenderer did not respond to the question or the response wholly failed to demonstrate an ability to meet the sub-criteria requirement. **Any proposal marked as a Fail will be excluded from the competition.**

Calculation of total score

The below worked example shows how the tender total score will be calculated.

The winning tender is the one with the highest weighted value for money index. In the event of a tie-break between suppliers for the highest score, the tie supplier with the highest technical mark will be awarded the contract.

Weighted Value for Money Index example

The overall tender core is calculated as follows:

$$\frac{\text{Technical score}^{60/40}}{\text{Cost}}$$

Tender	Technical Score	Cost (£)	Weighted VFM Index	Rank
A	$21^{60/40} = 96.23$	40000	0.00241	
B	$27^{60/40} = 140.30$	50000	0.00281	
C	$18^{60/40} = 76.37$	45000	0.00170	

Weighted VFM Index is rounded to three significant figures.