Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

Contents

1. Background

1.1 The Joint Maritime Security Centre (JMSC) is the UK's centre of excellence for maritime security with a global reach. The Buyer is a cross-Government, multi-agency, joint civil-military organisation that is threat agnostic and provides Maritime Domain Awareness and Understanding (MDAU) in partnership with the Royal Navy's Maritime Domain Awareness Programme (RNMDAP), to all of government and UK law and marine-enforcement agencies. This is enhanced through the delivery of strategic assessments. In addition, the Buyer provides comprehensive operational coordination and coherence, which enables both effectiveness and efficiency in multi-agency responses to maritime security threats in UK home waters, the Overseas Territories or globally.

1.2 Surveillance of the maritime domain for UK security requires a multi-layered approach. The Buyer has recently commissioned a report, which has identified [redacted] which together will improve the UK's MDAU, [redacted] The Buyer's ambition is to integrate as many [redacted] to allow the creation and continuous evolution of the coherent MDAUMDA picture. Not only does this require design, delivery and life-cycle management of [redacted] services, but a comprehensive user experience plan and ongoing performance analysis to ensure the full benefits are being delivered for the nation.

1.3 The Buyer delivers accurate maritime situational awareness and understanding in near-real time. [redacted] for use within JMSC and across Government.

1.4 As part of creating and maintaining a comprehensive MDAU picture, the Buyer wishes to establish a contract for a service to deliver agile development and user-centred design services to accelerate digital and data innovation within JMSC. The outcomes will be a range of new or improvements to existing digital maritime security capabilities.

2. Service Requirements

2.1 The Supplier shall deliver one digital workstream (Workstream 1) with one additional workstream being optional for the Buyer (Workstream 2), in order to improve the Buyer's ability to monitor and analyse activity [redacted]

- Workstream 1: Maritime C5ISR Digital Tools and Data Layers

- Workstream 2: User Experience Design

2.2 The service is to be delivered by one Supplier as a single lot. The requirement has been divided into two workstreams, in order to emphasise the different

types of outcomes, and therefore the different skillsets that the Supplier shall demonstrate in their bid. Workstream 2 is currently intended to be delivered internally by the Buyer. However, Bidders are required to include rate card pricing for any Workstream 2 roles in their proposal as part of their overall submission. Should the Buyer require supplementary support or if a change in approach becomes necessary, the Supplier may be called upon to execute this portion of the work.

2.3 The Supplier shall provide the Buyer with a call-off mechanism against a zero-volume commitment contract to deliver a service which can provide a range of digital outcomes (see paragraph 2.5), [redacted] Due to the agile nature of digital development in JMSC, both workstreams will be divided into smaller, discrete, phases of work. As such, detailed outcomes will be defined in specific Statements of Work (SOWs), aligned to sprints. [redacted] Specific SOWs will be released to the Supplier over the duration of the contract and there is no guarantee of volumes of work under this requirement (zero-volume commitment) or a minimum spend by the Buyer. The scope is centered on Workstream 1 and encompasses a range of potential outcomes; however, contract utilisation will be subject to the Buyer's specific requirements. There is also no guarantee of the Buyer utilising this contract for Workstream 2.

2.4 The Supplier must be able to demonstrate a track record of delivering digital services within a maritime security, or similar, environment (Stage 1 – Shortlisting).

2.5 **Workstream 1: Maritime C5ISR Digital Tools and Data**

2.5. In Workstream 1 the Supplier shall deliver [redacted] (set out in paragraph 2.5.4) to improve Maritime Security, through situational awareness for the Buyer's stakeholders. The resulting outcomes must be:

a) [redacted]

d) Analysis of digital performance and recommendations for iterative improvement.

2.5. The Supplier shall delivers the following outputs, to support the outcomes listed above:

a) Translation of end-user needs (both the Buyer and cross-Government/agency partner subject matter experts) to develop technical requirements,

b) Prioritisation of sprint cycles to ensure appropriate burndown of the backlog,

c) Development of business cases (including financial plan, benefits, commercial route to market), delivery plans and risk mitigation plans t[redacted]

d) Management of the relationship with the third-party application/[redacted]

e) Liaison with the providers of the existing system (e.g. RNMDAP or others), in order to integrate [redacted] or improve the functionality or user experience of the existing system,

f) Successful delivery of the product, such as new [redacted] and

g) Development of suitable through-life performance mechanisms to enable the Buyer to understand the on-going and real-time quality [redacted]

h) Delivery of appropriate training to the end user.

2.5. The Supplier shall liaise between the [redacted] and the Buyer's database provider (currently RNMDAP) at an appropriate technical level to facilitate successful information exchange. The Buyer typically requires data in JavaScript Object Notation (JSON) format. It is also likely that data feed suppliers will have Application Programming Interface (API) based data sharing architecture, [redacted] and the Buyer's database provider (currently RNMDAP) [redacted] The Supplier shall determine and manage the [redacted] suppliers to meet these requirements, ensuring that all necessary [redacted] included.

2.5. [redacted]

a) [redacted]

[redacted]

5

j) [redacted]

[redacted]

[redacted]

2.5. Existing systems have already been developed by third parties (RNMDAP, or external providers), and therefore the Buyer does not require the Supplier to provide their own bespoke [redacted], but the Supplier shall work with the Buyer's stakeholders to identify, and then carry out the work in order to acquire targeted maritime domain awareness [redacted], and requirements for improvements to user experience and functionality, which can then be integrated into an existing solution via RNMDAP's in-house team. PAs such, the Supplier shall be responsible for [redacted] of the service, but not the actual technical build/change.

2.5. The Supplier shall have an awareness of National Cyber Security Centre doctrine and experience in employing cyber security policy in delivery of projects.

2.5. The Supplier shall provide resources for Workstream 1 which are:

[redacted] (Supplier to determine for each SoW).

2.6 **Workstream 2: User Experience Design**

2.6. The Supplier shall develop a Maritime Security user experience design and development plan with detailed user requirements, including (but not limited to):

) Persona, use case and user story creation,

) Issue triage, feature discovery and sprint backlog development, and

) User acceptance and validation criteria definition.

2.6. All of Supplier's typical outputs to be report-based, and all IP will remain with the Buyer (Call-Off Schedule 6 – Intellectual Property Rights and Additional Terms on Digital Deliverables).

2.6. The Supplier shall deliver:

a) A long-term (c. 10 year) high-level user experience design plan,

b) Updates and iterates of the user requirement analysis over the lifetime of the contract, to respond to adjustments in maritime security policy, and

c) Specific stand-alone user-experience work packages to support on-going the Buyer's digital capability development.

2.6. The Supplier shall provide resources for Workstream 2 (if required) which are:

a) Projected to be up to [redacted] per year (Supplier to determine for each specific SoW issued).

3. User Types

3.1 **Joint Maritime Security Centre**

3.1.1 The Buyer is the UK's centre of excellence for maritime security with a global reach. It is a cross-Government, multi-agency, joint civil-military organisation that is threat agnostic. Joint Maritime Security Centre has [redacted] core teams [redacted], plus partner agencies and organisations.

3.2 **Other Government Departments and Agency Partners**

3.2.1 The Buyer offers government departments and UK law- and marine-enforcement agencies a central point of UK maritime expertise and understanding to assist policy and decision making. As well as delivering strategic advice and operational support, the Buyer also shares [redacted] with partners across Government, which provides value-for-money for the taxpayer.

3.3 In **Workstream 1** the Supplier shall engage with the Buyer and broader Government stakeholders to refine the detailed user requirement for the [redacted] This engagement work shall be done via a combination of workshops and individual meetings, depending on the scale of the work package.

3.4 In **Workstream 2** the Supplier shall engage across the maritime security system community in order to develop detailed, long term, whole system user experience requirements. This includes stakeholders from, but not limited to, Cabinet Office, COBR, Border Force, Police, DESNZ, DEFRA, Marine Management Organisation, DfT, Maritime & Coastguard Agency, HM Coastguard, MoD, Royal Navy, HM Treasury, FCDO. We envisage this engagement work being done via a combination of workshops and individual meetings, depending on the scale of the work package. This workstream is currently being delivered internally. Bidders are required to include pricing for relevant roles in their proposal (see Financial Pricing Model), as part of the overall submission. Should the internal team require supplementary support or if a change in approach becomes necessary, the Bidder may be called upon to execute this portion of the work.

4. Security

4.1 The Supplier shall provide (or sub-contractor, if appropriate) personnel working on the delivery (not support) of the Contract, this personnel must hold valid Security Check (SC), as a minimum.

4.2 Specific Statements of Work may require Developed Vetting (DV) personnel. This will be made clear as part of the SoW. As a result, the Supplier shall be able to provide DV cleared individuals.

4.3 [redacted].

5. Standards & Certifications

5.1 The Supplier shall demonstrate their ability to conform to the following standards and hold the following certifications:

a) ISO9001 Quality Management
b) ISO27001 Information Security Management
c) Web Content Accessibility Guidelines
d) National Institute of Standards and Technology (NIST) Cyber Security Framework
e) National Cyber Security Centre (NCSC) Cloud Principles
f) Cyber Essentials

6. Location and Working Arrangements

6. The Supplier shall provide people who can attend in-person meetings with the Buyer, the Royal Navy Maritime Domain Awareness (RNMDA) team, and others as appropriate at JMSC, [redacted] as required to enable requirements understanding, stakeholder management, and working at the appropriate classification (the current expectation is [redacted] SoW, depending on the specific deliverable, but is subject to change).

6. In accordance with Call-Off Schedule 5 (Pricing Details and Expenses Policy), any persons from the Supplier who attend meetings at PTP will not be eligible for having travel expenses paid, but travel to meetings [redacted] as part of contracted work can be reclaimed subject to the limitations and approvals in accordance with Home Office Policy, which will be shared with the

successful Supplier on commencement of the contract (Call Off Schedule 5 - Pricing Details and Expenses Policy).

7. Contract Term & Price

7. The contract term shall be for an initial period of two (2) years, with one (1) optional extension period of one (1) year, at the Buyer's sole option.

7. The total budget value for this contract is £4m ex.VAT, covering a duration of two (2) years, with an option to extend for an additional one (1) year.

7. The total budget value for Workstream 1 is £3m ex.VAT and the total budget value for Workstream 2 is £1m ex.VAT.

7. This contract shall create a call-off mechanism subject to a zero-volume commitment for the provision of services as outlined above. Please be aware that this contract does not guarantee any specific volume of services or assured payments.

7. The first Statement of Work for Workstream 1 shall be fully mobilised, with all personnel ready to commence work no later than stated in Volume 1 – Instructions to Bidders.

8. Definitions / Abbreviations

Term	Definition
Application Programming Interface (API)	A set of protocols, tools and definitions that allow different software applications to communicate and interact, often used in maritime security systems for data integration and automation.
Automatic Identification System (AIS)	A maritime communication system used for tracking and identifying vessels in real time, transmitting location, speed, and other navigational data to improve situational awareness and security at sea.
Buyer (the Buyer)	The public sector purchaser identified as such in the Order Form. This is the Secretary of State for the Home Department acting through Border Force.
Bidder	An organisation which is invited to submit a Tender Response.
Contract	The contract between the Buyer and the successful Supplier, which consists of the terms set out and referred to in the Order Form.

Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR)	A framework used in defence and security sectors to integrate information gathering, analysis, and decision-making to support operations.
Developed Vetting (DV)	Level of security clearance in the UK, required for individuals with substantial access to sensitive information or classified information.
Digital Maritime Security Capabilities (DMSC)	Digital Maritime Security Capabilities the programme, as being referred to in these tender documents.
Electronic Source Intelligence (ELINT)	The collection and analysis of electronic signals, such as radar and radio frequencies to monitor, detect and assess threats in maritime security operations.
Exclusive Economic Zone (EEZ)	Exclusive Economic Zone as defined under the 1982 United Nations Convention on the Law of the Sea.
Freedom of Information Act 2000 (FOIA)	Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation
Financial Pricing Model (FPM)	A mathematical model used to determine the cost of products or services based on various factors such as risk, volumes, and costs. Applied in the evaluation of price for DMSC (Volume 5 – Financial Pricing Model).
Find a Tender Service (FTS)	The UK's official online platform for publishing public sector contract notices, replacing EU's OJEU system post-Brexit.
Government Security Classification (GSC)	The UK government's system for classifying sensitive information into categories such as OFFICIAL, SECRET and TOP SECRET.
Invitation to Tender (ITT)	A formal procurement document issues to potential suppliers, inviting them to submit bids for a contract.
JavaScript Object Notation (JSON)	A lightweight data-interchange format used for structuring data, commonly applied in web and maritime security applications for efficient data exchange.
Joint Maritime Security Centre (THE BUYER)	Joint Maritime Security Centre, also specified as the "Buyer".
Key Performance Indicator (KPI)	A measurable value used to evaluate the success of an individual, project or organisation in achieving key objectives.

Long-Range Identification and Tracking (LRIT)	A global system mandated by the IMO to track and monitor vessels remotely, enhancing maritime domain awareness security.
Maritime Domain Awareness (MDA)	The effective understanding of activities in the maritime environment that could impact security, safety, economy or the environment.
Maritime Domain Awareness and Understanding (MDAU)	A broader concept of than MDA, incorporating intelligence, surveillance, and decision-making to enhance maritime security and operations.
Most Economically Advantageous Tender (MEAT)	A procurement approach that evaluates tenders based on a combination of price and quality to achieve best value for money.
Non-Collusion Certificate	Also known as a certificate of bona fide tendering, declaration by Bidders in a tender process confirming that they have not engaged in anti-competitive practices.
National Cyber Security Centre (NCSC)	A United Kingdom Government agency responsible for improving cybersecurity resilience and protecting critical national infrastructure, including maritime security systems.
National Institute of Standards and Technology (NIST)	A U.S. agency that develops and promotes cybersecurity standards, guidelines and best practices, including frameworks applicable to maritime and digital security.
Open-Source Intelligence (OSINT)	Collection and analysis of publicly available information from sources such as websites, social media, and government reports to enhance maritime and cybersecurity situational awareness.
Portsdown Technology Park (PTP)	A UK Ministry of Defence site specialising in advanced technology research and development, particularly in defence and maritime domains.
Prior Information Notice (PIN)	A notice published by a public sector organisation to inform potential suppliers about upcoming procurement opportunities before the formal tender process begins.
Regulations (PCR 2015)	Public Contracts Regulations 2015 (as amended).)
Royal Navy Maritime Domain Awareness (RNMDA)	The Royal Navy's framework for monitoring and understanding activities in maritime areas of interest to enhance operational effectiveness and security.
Security Check (SC)	A UK government security clearance lever required for individuals accessing sensitive information, but at a lower level than Developed Vetting (DV).

Statement of Work (SOW)	A detailed document outlining scope, objectives, deliverables, and requirements of contracts or project.
Tender Response	A tender submitted by the Bidder to the Buyer and annexed to or referred to in Schedule 4 (Tender).
Total Evaluated Price (TEP)	The final cost assessment of a tender submission, incorporating both the base price and any additional cost factors as per evaluation criteria.
Timetable	The timetable for the procurement set out in section 4 of these instructions.
Transfer of Undertakings (Protection of Employment) (TUPE)	Transfer of Undertakings (Protection of Employment) Regulations 2006 (as amended).
Vessel Monitoring System (VMS)	A satellite-based tracking system used by maritime agencies to monitor and regulate vessel movements for security and compliance.