DPS Schedule 6 (Order Form and Order Schedules)

Order Form

ORDER REFERENCE:	**TTSC3049**
THE BUYER:	**Department for Transport**
BUYER ADDRESS	**33 Horseferry Road, London SW1P 4DR,**
THE SUPPLIER:	**Actica Consulting Limited**
SUPPLIER ADDRESS:	**4 Stirling House, Guildford, Surrey, GU2 7RF**
REGISTRATION NUMBER:	03396854
DUNS NUMBER:	520304304

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 10 August 2022. It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
Non-assured NCSC Services, Risk Assessment, Certification (e.g. Cyber Essentials), Security Supply Chain Analysis, Threat Intelligence, Clearance: Counter Terrorist Check, Transport, Water, Coast Guard

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

- Joint Schedules for RM3764iii
  - o Joint Schedule 2 (Variation Form)
  - o Joint Schedule 3 (Insurance Requirements)
  - o Joint Schedule 4 (Commercially Sensitive Information)
  - Joint Schedule 6 (Key Subcontractors)
  - Joint Schedule 7 (Financial Difficulties)
  - Joint Schedule 8 (Guarantee)
  - Joint Schedule 10 (Rectification Plan)

- Order Schedules for RM3764iii

  - Order Schedule 4 (Order Tender)
  - Order Schedule 5 (Attachment 5 - Pricing Details)
  - Order Schedule 20 (Attachment 3 - Order Specification)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:

None

ORDER START DATE: 10 August 2022

ORDER EXPIRY DATE: 31 March 2023

ORDER INITIAL PERIOD: 31 March 2023

ORDER OPTIONAL EXTENSION Optional extension of 3 additional months

DELIVERABLES

See details in Attachment 3 (Schedule 20 Order Specification)

MAXIMUM LIABILITY
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £69,200

ORDER CHARGES
Attachment 5 Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD

Suppliers must be in possession of a written purchase order (PO), before commencing any work under this contract. You must quote the aforementioned PO number on all invoices, and these must be submitted directly to:

ssa.invoice@sharedservicesarvato.co.uk

or via post to:

Accounts Payable,
Shared Services arvato,
5 Sandringham Park,
Swansea Vale,
Swansea
SA7 0EA

Invoices received without the correct PO number will be returned to you and will delay receipt of payment.

BUYER'S AUTHORISED REPRESENTATIVE
Commercial:
[redacted]

Contract Manager:
[redacted]

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

[redacted]
Address: 4 Stirling House, Stirling Road, Guildford, Surrey, GU2 7RF

SUPPLIER'S CONTRACT MANAGER
[redacted]
Address: 4 Stirling House, Stirling Road, Guildford, Surrey, GU2 7RF

PROGRESS REPORT FREQUENCY
First draft report for comment by participants no later than 31/01/2022

PROGRESS MEETING FREQUENCY
Weekly update via email to raise any issues for the project going forward

KEY STAFF
[redacted]
Address: As above

KEY SUBCONTRACTOR(S)
Not applicable

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Not applicable
ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments made in the Suppliers tender response to the Social Value evaluation criteria.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:		Name:	
Role:	Company Secretary	Role:	Commercial Relationship Manager
Date:	11/08/2022	Date:	16/08/2022

ORDER SCHEDULE 20: ORDER SPECIFICATION

1.1 Title

1.1.1. To update the Code of Practice, Cyber Security for Shipping guidance published in 2017.

2. Purpose

2.1.1. To update the existing Guidance: Code of Practice, Cyber Security for Ships to ensure it is concurrent with cyber threat to the maritime domain, vessels and companies. The product produced from this project will replace the current DfT cyber shipping guidance, and provide industry with a coordinated and updated UK government referenced product. The final contract deliverable will include a threat assessment of organised criminal activity, hacktivists, and state threat actors, which could affect the maritime industry. This will included a cyber framework which provides an overview of what to look out for, how a cyber-attack could transpire in the maritime domain, migrating actions and best practise that industry should consider in alignment with IMO regulations, and assists them in a company's or ship's overall risk management system and subsequent business planning for cyber security practices in a report form.
2.1.2. In 2017, the Department for Transport (DfT), DSTL and IET published Cyber Security Code of Practice for ships.
2.1.3. The Code of Practice aimed to set out why it is essential that cyber security be considered as part of a holistic approach throughout a ship's lifecycle, as well as setting out the potential impacts if risks are not mitigated. The Code of Practice was intended to be used as an integral part of a company's or ship's overall risk management system and subsequent business planning, to ensure that the cyber security of the ship, or fleet, is managed cost effectively as part of mainstream business. The code of practice served as a 'best management practice'.

2.1.4. The purpose of this project is to ensure UK maritime industry takes the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping. It is essential to keeping shipping cyber security guidance up-to-date and relevant to ensure the maritime industry has a resilient cyber security and risk management capability and are in step with changes to international regulations.
2.1.5 The benefits to industry are significant – the current guidance for British flag shipping is from 2017 and is outdated and does not represent current cyber-attacks targeted towards the shipping industry. The project is essential to ensure the maritime industry has a resilient cyber security and risk management capability and is in step with changes to international regulations. There is a vacuum between flag state guidance, IMO cyber regulations, audit principles for MCA and other registries and international associations. The UK flag, as managed by the MCA, is number one in the Paris group for quality – we need to ensure the 'offer' from the flag state isn't diminished because we have no meaningful cyber security guidance. This will also help us achieve our short-term recommendations for M2050.

3. Background to the Contracting Authority

3.1.1. The contracting authority is the Department for Transport (DfT). DfT is the government department responsible for the safety and security of transport across the UK, including security for UK flag vessels.
3.1.2. Transport Security, Resilience and Response (TSRR) Directorate within DfT leads on national security matters, ranging from counter terrorism and cyber security to planning for and responding to natural hazards or civil contingencies. The Cyber Security team is responsible for identifying and helping to counter cyber security threats in the transport sector.

4. Background to Requirement

4.1.1. The maritime sector is a vital part of the global economy, whether it is carrying cargo, passengers, or vehicles. Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life.
4.1.2. Poor cyber security could lead to significant loss of customer and/or industry confidence, reputational damage, potentially severe financial losses or penalties, and litigation affecting the companies involved. The compromise of ship systems may also lead to unwanted outcomes, for example:

4.1.3 Physical harm to the safety system, the shipboard personnel or cargo – in the worst-case scenario this could lead to a risk to life and/or the loss of the ship.

4.1.4. Disruptions caused by the ship no longer functioning or sailing as intended.

4.1.5. Loss of sensitive information, including commercially sensitive or personal data.

4.1.6. Permitting criminal activity, including kidnap, piracy, fraud, theft of cargo, imposition of ransomware.

4.1.7. Social Value will be applied by this project within the Wellbeing theme. It is important that all staff have the correct training to manage the cyber security risks associated with their jobs as the emotional impact of causing a breach can be significant. Staff feeling equipped to deal with different situations is a key enabler to wellbeing and feeling in control of your environment.

5. Definitions

Expression or Acronym	**Definition**
CCS	Crown Commercial Service
NCSC	National Cyber Security Centre
Buyer	Department for Transport
DSTL	Defence Science and Technology Laboratory
IET	Institution of Engineering and Technology

Expression or Acronym	Definition
IMO	International Maritime Organisation
MCA	Maritime and Coastguard Agency
CAF	Cyber Assessment Framework

6. Scope of Requirement

6.1.1. The Department is willing to facilitate official information from government sources if required for this project.

The following actions are in scope:

6.1.2. Reviewing and updating the current set of guidance for industry.

6.1.3. Meeting manufacturers and operators of shipping equipment to review current guidance.

The following is not in scope:

6.1.4. Coordination with the National Cyber Security Centre (NCSC) and regulatory bodies; these organisations will be able to feed into the project through supporting the DfT.

7. The Requirements

7.1.1 The guidance will be an update to the 2017 Cyber Security Code of practice for ships. This update will specifically need to focus on changes since 2017 in the threats to international shipping from cyber-attack. It will also include an updated threat assessment including from hostile state actors and the principle cyber-attack methods used.

7.1.2. The expected project output will be an updated Code of Practice document which covers the following:

7.1.3. Updates to cyber regulations since 2017 – this will take into account IMO Resolution MSC.428(98) which requires ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system (since Jan 2021); the guidance must bring together in one place all the relevant guidance for shipping cyber security.

7.1.4. A new Cyber Assessment Framework (CAF) ‘lite’ assessment. The NCSC’s CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. We seek to create a ‘lite’ version to help organisations consider their cyber security posture. This CAF lite will be in the form of an assessment/checklist that will provide shipping organisations with advice to ensure they are compliant with IMO’s regulations and UK best practice.

7.1.5. A study of standards including standards ISO27001 and National Institute of Standards and Technology’s cyber guidance to determine whether any of this guidance could be reflected in the output from this project.

7.1.6. An updated and expanded section covering a number of real-life case studies demonstrating why cyber security is important to shipping.

7.1.7. An updated section on threat and vulnerability which sets out the cyber risk from all threat actors including Hostile State Actors, Serious Organised Crime Groups and others

7.1.7.1. Set out a risk matrix on the priority of threats to ship cyber security from all actors

7.1.7.2. Outline the different methods actors could use to infiltrate shipping systems and provide best practice for mitigation against the main types of attacks

7.1.7.3. Outline the risks created from vulnerabilities within onboard ship systems

7.1.8. Information on available cyber security software products including an update to available software since the 2017 guidance and technical skills required to use and keep these products up-to-date.

7.1.9. Addition of a section that covers Remotely Operated and Autonomous Vessels. This should include the additional risks introduced by remote operations and autonomy compared to conventional vessels and the impact of using Remote Operation Centres on operation arrangements.

7.1.10. A section on guidance on how a shipping company should respond to a cyber security incident including immediate actions and who to contact.

8. Key milestones and deliverables

8.1.1. The following Contract milestones/deliverables shall apply.

8.1.2. Reports and updates shall be in written in an accessible format in accordance with gov.uk guidelines, with all tables, figures, charts and images clearly described.

Milestone/Deliverable	Description	Timeframe/ Delivery Date
1 - Milestone	Kick-Off meeting to run through approach and formally start the work.	Within week 1 of Contract Award
2 - Milestone	Progress updates to raise any issues, confirm contact details of participants, note any changes, etc.	Within week 6 of Contract Award
3 - Deliverable	Briefing session to update on: Required regulatory updates and updates to standards Case studies New security software review	No later than: 31/10/2023

Milestone/Deliverable	Description	Timeframe/ Delivery Date
4 - Deliverable	Briefing session to update on: Threat and vulnerabilities assessment Risks to autonomous ships and remote operating centres 'CAF lite'	No later than: 31/12/2022
5 - Deliverable	Draft code of practice product for comment by participants	No later than: 31/01/2023
6 - Deliverable	Final code of practice product delivered	No later than: 31/03/2023

9. Management Information and Reporting

9.1.1. Reporting on project status/progress via a series of meetings by the Supplier will be provided as a minimum on a weekly basis and will be made available to the contract manager two working days before the contract review meetings.

10. Volumes

10.1.1. This contract is a one-off requirement via the Cyber Security Services 3 Dynamic Purchasing System for full completion by 31 March 2023. The supplier will grant the Authority the option of an extension to the contract up to 3 months, which the Authority may take up, providing written notice of a variation to the contract within 1 month of its expiry date.

11. Continuous Improvement

11.1.1 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

12. Environment, Sustainability and Social Value

12.1.1 The supplier shall demonstrate how they work will support the wellbeing, including physical and mental health, in the shipping industry.

13. Payments and Invoicing

13.1.1 The Supplier shall provide a firm cost price for this work.
13.1.2. The Supplier shall provide a capped cost price for this work. The maximum allocated budget for the contract is **£70,000** excluding VAT. Bids above this value may be discounted at the discretion of the DfT.
13.1.3. To note, 20% of the total evaluation score will be allocated to evaluation of the prices tendered for the specified requirement.
13.1.4. Prices are to be submitted via DfT's E-Sourcing portal. The portal is available using the following link: https://dft.app.jaggaer.com/web/login.html

14. Quality

14.1.1.The Supplier shall state how they will ensure a quality product and provide Quality Assurance through the provision of a Quality Plan. They may provide a summary of the Quality Assurance arrangements, principles, standards and checks they will use within the project.
14.1.2. The Supplier shall have Cyber Essentials plus certification and proof will be required once the contract has been awarded.

15. Staff and Customer Service

15.1.1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
15.1.2. The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
15.1.3. The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
15.1.4. The Supplier shall have two years' experience working with or on projects relating to Transport Critical National Infrastructure.
15.1.5. The Supplier shall have at least three years GDPR experience.

16. Service Levels and Performance

16.1.1. The Authority will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA Description	Target
1	Progress Report	Progress reports will be supplied to the DfT project manager by phone or email (to be confirmed). This will include a summary of progress against the delivery.	Weekly
2	Risk monitoring	The Supplier will raise any concerns about the possibility of failing to meet the overall deadline and lack of relevant information to meet the requirements.	Weekly
3	Communication	The Supplier shall acknowledge any communications from the contract/project manager within 2 working days	2 working days
4	Emergencies	If there is an urgent issue, the Supplier shall make the contract manager aware of this within 2 working days	2 working days

16.1.2. If the Supplier is unable to provide a product to the agreed quality within the specified time the Authorities reserves the right to retain payment, either in whole or in part.

17. Security and Confidentiality Requirements

17.1.1 The Supplier must be able to handle and store classified material up to and including OFFICIAL SENSITIVE level. The project reports and guidance for government and industry will be classified at OFFICIAL SENSITIVE.
17.1.2. As a minimum staff should have or be willing to apply for and obtain the Baseline Personnel Security Standard (BPSS) and must state this explicitly in their bid. Proof of security clearance for all staff involved in this project will be required once the contract has been awarded.
17.1.3. The Supplier should demonstrate the measures in place to keep this information secure. Specifically, in the bid document the Provider should provide detail on how they will meet the following requirements:

17.1.4. Information classified at OFFICIAL SENSITIVE level relating to this project should only be communicated electronically with those contacts provided by the DfT using the methods below.

17.1.5. The Supplier should ensure the security of the information in transit. Electronically this will involve using software (for example Egress Switch system) to encrypt the files, preferably using AES-256, or other measures that offer an equivalent level of protection.

17.1.6. Any passwords used to encrypt files should be complex and should be conveyed separately to the files themselves.

17.1.7. Any electronic files should be stored on an IT system that has access controls that only allow approved and cleared personnel with a genuine 'need to know' to access them to read and copy. The IT system should be protected by an appropriate firewall.

17.1.8. Once electronic files are no longer needed, they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.

17.1.9. Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL SENSITIVE and numbered to ensure no copies are lost. Paper and printed material should be shredded when no longer needed.

17.1.10. If any paper copies are to be posted, advice should be sought from DfT.

17.1.11. Access to all material generated by this project (including source data supplied by DfT) must be on a limited and controlled basis, by persons approved by the DfT.

17.1.12. Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act 2018.

17.1.13 Further information on security classification is available on the Cabinet Office website at the following addresses:
http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-personnel-security-controls.pdf
https://www.gov.uk/government/publications/security-policy-framework

The Supplier shall have Cyber Essentials plus certification and proof will be required once the contract has been awarded.

18. Contract Management

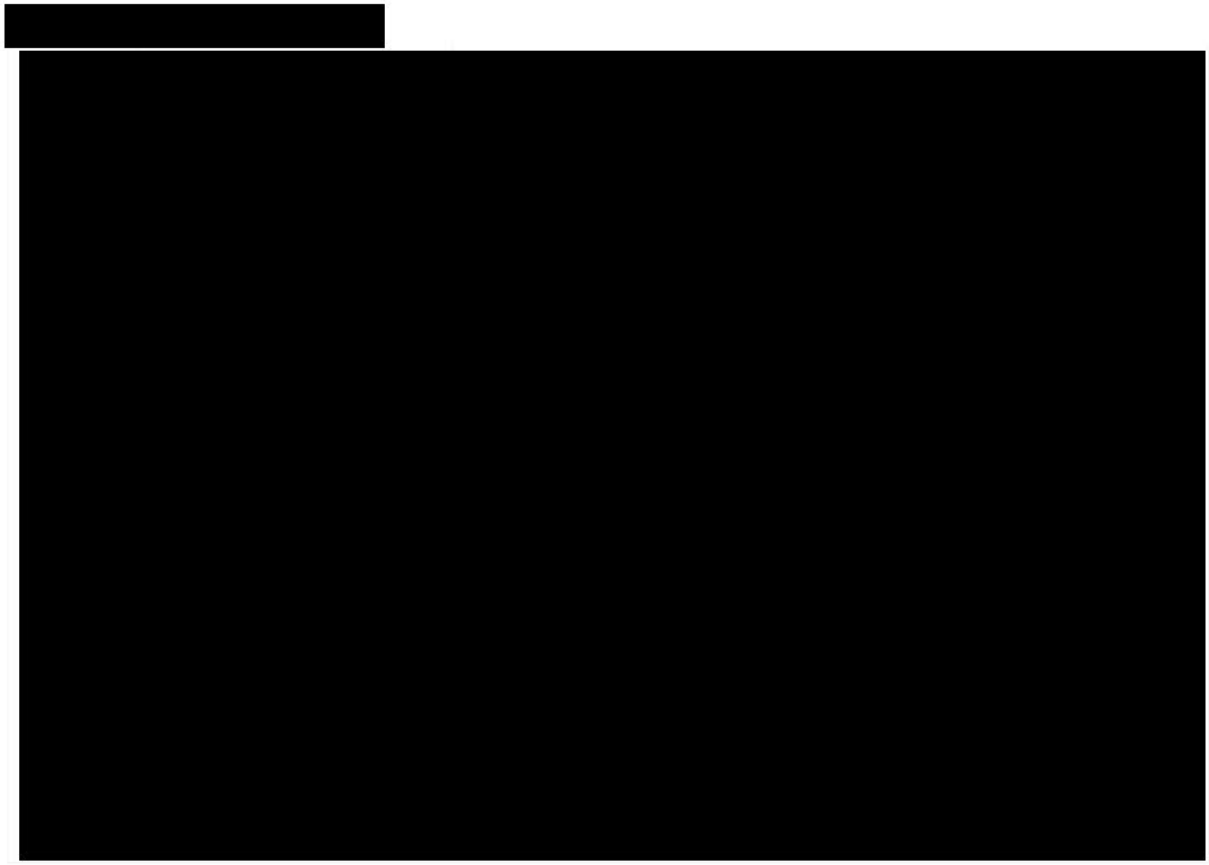
18.1.1. Attendance at Contract Review meetings shall be at the Supplier's own expense

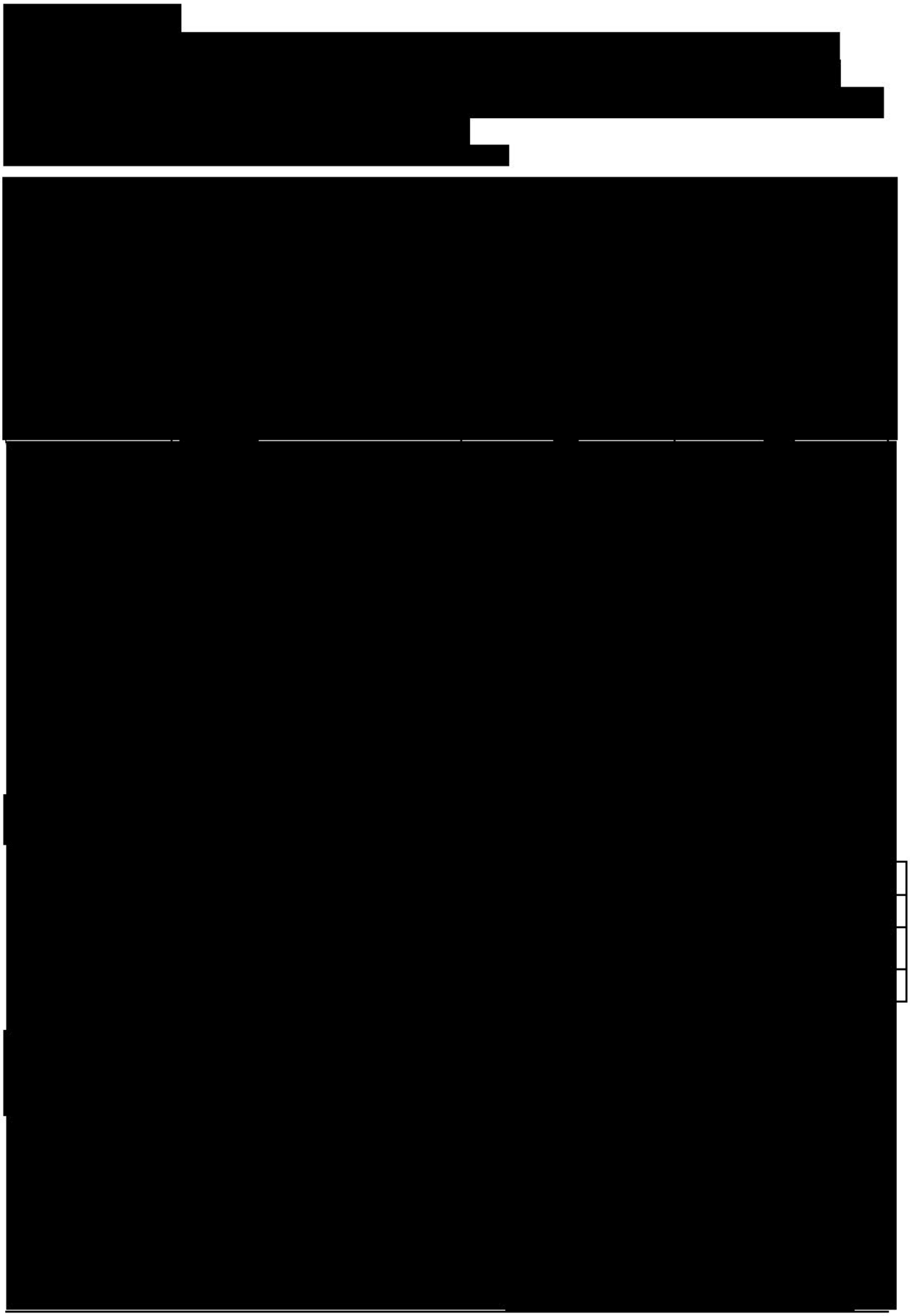
19. Location

19.1.1. The location of the Services will be carried out at the Supplier's premises within the UK. Any anticipated travel and expenses incurred from engagement with stakeholders, or the Authority must be included in the bid price.

ORDER SCHEDULE 4: ORDER TENDER

[redacted]





ORDER SCHEDULE 5: PRICING DETAILS