CONTENTS

[1. PURPOSE 2](#_Toc444518866)

[2. BACKGROUND TO THE CONTRACTING aUTHORITY 2](#_Toc444518867)

[3. Background to requirement/OVERVIEW of requirement 2](#_Toc444518868)

[4. definitions 3](#_Toc444518869)

[5. scope of requirement 3](#_Toc444518870)

[6. The requirement 4](#_Toc444518871)

[7. key milestones 5](#_Toc444518872)

[8. authority’s responsibilities 5](#_Toc444518873)

[9. reporting 5](#_Toc444518874)

[10. volumes 5](#_Toc444518875)

[11. continuous improvement 6](#_Toc444518876)

[12. Sustainability 6](#_Toc444518877)

[13. quality 6](#_Toc444518878)

[14. PRICE 6](#_Toc444518879)

[15. STAFF AND CUSTOMER SERVICE 6](#_Toc444518880)

[16. service levels and performance 6](#_Toc444518881)

[17. Security requirements 7](#_Toc444518882)

[18. intellectual property rights (ipr) 8](#_Toc444518883)

[19. payment 8](#_Toc444518884)

[20. additional information 9](#_Toc444518885)

[21. Location 9](#_Toc444518886)

# PURPOSE

## The term ‘Port Community System’ refers to an electronic platform that connects the multiple systems operated by a variety of organisations that make up a seaport community. It is shared in the sense that it is set up, organised and used by organisations in the same sector.

## The purpose of the work is to assess the extent to which UK ports depend on third party common data systems; which suppliers and systems are the most critical to the maritime sector; and to assess the potential impacts from their loss caused by a compromise of data/service provider’s network and information systems. The work will increase the Government’s understanding of how dependent the sector and individual organisations are on third party common data systems, and the potential impact if these systems were adversely affected by any cyber-related incident. The resulting reports will also recommend the next steps for government departments and industry to take.

## The Government-facing report will be used within the Department for Transport (DfT) and shared with the National Cyber Security Centre (NCSC), Defence Science and Technology Laboratory (DSTL), the Marine Accident Investigation Branch (MAIB) and the Marine and Coastguard Agency (MCA) to inform policy development in this field. The industry-facing report will be shared with participants in the study, as well as other critical operators.

# BACKGROUND TO THE CONTRACTING aUTHORITY

## 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. DfT also has a responsibility for maritime security which covers sea and air ports.

# Background to requirement/OVERVIEW of requirement

## Like much of the UK’s Critical National Infrastructure (CNI), the UK maritime sector is a potential target for cyber-attacks and victim of other information security incidents. These may occur across the multitude of different systems and technologies that facilitate trade & travel. There is scope for considerable economic and social disruption from malicious attacks, with the maritime sector being an attractive target for organised crime groups.

## There is a shortage of understanding of the dependencies of UK ports on common third party data systems and the impact of the loss or compromise of these systems on the effective operation of the ports. DfT and the DSTL have previously conducted studies into port cyber security which provided some insights and a high level view of how a CNI port depends on this data and the way it is ingested. The NCSC has also identified that there is a lack of knowledge of Port Community Systems.

## The outputs from this work should enable DfT to have a significantly improved view of the risk in this area and the maturity of industry’s resilience plans, providing strong options for further work if needed. This will assist DfT in developing a high level risk picture with which to inform senior officials and Ministers who have taken an interest in how the maritime industry is tackling this potential risk.

## Proposals will be evaluated on the basis of demonstrable understanding of both the maritime industry and cyber security issues; how comprehensive the plan for engaging with relevant stakeholders is; proven experience in the field of maritime, which should include experience of cyber security; the approach to the exchange and protection of the sensitive information that will be obtained and the cost forecast for the work.

# definitions

|  |  |
| --- | --- |
| Expression or Acronym | Definition |
| CNI | Critical National Infrastructure |
| CPNI | Centre for the Protection of National Infrastructure |
| DfT | Department for Transport |
| DSTL | Defence Science and Technology Laboratory |
| ENISA | European Network and Information Security Agency |
| MAIB | Marine Accident Investigation Branch |
| MCA | Marine and Coastguard Agency |
| NCSC | National Cyber Security Centre |
| PoF | Port of Felixstowe |

# scope of requirement

## The following items are in scope:

### The Potential Provider will need to engage and meet with at least ten UK ports. The Potential Provider must ensure they engage with some specific ports, the identities of which the Authority will inform the Potential Provider once the contract is awarded.

### The Potential Provider must engage and meet with at least two key industry service and data providers that provide services to UK ports. The Authority will specify specific service and data providers to the Potential Provider. Some of these third party providers may be based outside the UK so some international travel may be required.

### The Potential Provider will be required to investigate whether other systems, not specified by the Authority, are in use in UK Ports, and how widespread their use is.

### The following items are excluded from scope:

#### The Potential Provider will not be required engage with non-UK ports. This also means that the Potential Provider will not be required to engage with third party providers that only provide a service to non-UK

# The requirement

## A consultancy-based exercise to assess ports’ dependence on key data sources. The Potential Provider should engage with key industry partners including UK ports and the data/service providers. This will include arranging and travelling to meetings with appropriate staff members from the industry.

As well as assessing dependencies and potential impacts of a loss of data systems, the reports should provide an assessment of what steps are being taken to assure this data is protected, and the resilience plans that are in place.

In the reports, the Potential Provider will need to present the outcomes of the meetings with the industry partners along with assessments of the dependencies and impacts that are discussed.

The Potential Provider will need to write two electronic reports:

### One report will be written for Government and will outline what the most critical sources of data are, and the broad dependence of the ports on them to maintain effective operations (including the likely effectiveness of contingencies). The report will also highlight any potential impacts from loss of service due to a compromise of third party data provider’s networked and information systems. Potential causes of compromise or unavailability of systems to be considered should not be restricted to cyber-attacks, but should include physical damage to critical systems such as flooding and fire damage. The report should also provide next steps for government departments and industry partners to work together on the outcomes of the report. The report should further highlight any commonalities and variations in responses across the industry partners.

### The second report will broadly be the same as the first report, however it will be written for the maritime industry, including ports and the data/service providers, and therefore any references to individual organisations will need to be anonymised, and steps taken to ensure no stakeholder is able to be identified. The report should also provide good practice recommendations for the maritime industry and data/service provider to work together on the outcomes of the report.

## It is expected that Potential Providers should be able to demonstrate:

### Expertise in the fields of maritime, and evidence of how they would apply this to the project. This should include CV’s of the people undertaking the work, the time they are expected to put into the work, a list of previous relevant work and example case studies.

### The Potential Provider should outline their proposed approach of getting the evidence they need from industry partners.

### A detailed plan of how they will undertake the work and who within the team will do which parts. For the plan a case study should be used to demonstrate how the work will be conducted and a project plan for the steps involved. This includes plans for travel to engage with industry.

### The Potential Provider should also provide information on the resources and relationships they have available and how these will be utilised.

# key milestones

## The Potential Provider should note the following project milestones that the Authority will measure the quality of delivery against:

|  |  |  |
| --- | --- | --- |
| **Milestone** | **Description** | **Timeframe** |
| 1 | Inception meeting (Date to be agreed) | December 2017 (2 weeks from Contract Award) |
| 2 | Delivery of first draft of report |  February 2018 (9 weeks from Inception meeting) |
| 3 | Final report delivery and presentation |  March 2018 (4 weeks from Delivery of first draft report) |

# authority’s responsibilities

## The Authority will need to ensure that sign-off and comments on the final report are provided as per the agreed timetable.

## In order to ensure that industry partners are as open as possible in their engagement with the Potential Provider, the Authority will provide a covering letter to the Potential Provider. The letter will explain that two reports will be produced; one for DfT and NCSC which will not be shared beyond that group; and one to be shared with industry which will be anonymised to ensure no stakeholder will be identified. The letter will also explain the Authority will not take any regulatory or punitive action with individual organisations in response to the findings.

# reporting

## Please refer to the Potential Provider’s key reporting responsibilities as mentioned in 6.1.

# volumes

## This requirement is a one-off contract via Contracts Finder for an estimated fifteen week period from Wednesday 13th December 2017 to Friday 30th March 2018.

# continuous improvement

## 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.

# Sustainability

## Not Applicable.

# quality

## The Provider 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.

# PRICE

## The contractor shall provide a capped cost price for this work. The maximum allocated budget for the contract is £50,000.00 excl. VAT. Bids above this value may not be considered, at the discretion of the DfT.

## Prices are to be submitted via the e-Sourcing Suite (Appendix E) excluding VAT.

# STAFF AND CUSTOMER SERVICE

## The Authority requires the Potential Provider to provide a sufficient level of resource throughout the duration of the Understanding of Port Community Systems Contract in order to consistently deliver a quality service to all Parties.

## Potential Provider’s staff assigned to the Understanding of Port Community Systems Contract shall have the relevant qualifications and experience to deliver the Contract.

## The Potential Provider 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.

# service levels and performance

## The Authority will measure the quality of the Supplier’s delivery by:

### assessment of their progress alongside the agreed milestones set out in paragraph 7.2.

|  |  |  |  |
| --- | --- | --- | --- |
| 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. | Fortnightly |
| 2 | Risk monitoring | The Potential Provider 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 Potential Provider 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 Potential Provider shall make the contract manager aware of this within 2 working days. | 2 working days |

## In the event that the Provider 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.

# Security requirements

## The Provider must be able to handle and store classified material up to and including OFFICIAL SENSITIVE level. The project report will be classified at OFFICIAL SENSITIVE.

## 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.

## The Provider 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:

### Information classified at OFFICIAL SENSITIVE level relating to this project should not be communicated electronically, except between the contractor and DfT (and other parties approved by DfT) and then only using the methods below.

### The Potential Provider 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.

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

### Any electronic files should be stored on an IT system that has access controls that only allow approved personnel with a genuine ‘need to know’ to access them to read and copy. The IT system should be protected by an appropriate firewall. This also applies to data stored offshore.

### 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. This also applies to data stored offshore.

### 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.

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

### Access to all material generated by this project (not included source data unless supplied by DfT) must be on a limited and controlled basis, by persons approved by the DfT.

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

## 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>

# intellectual property rights (ipr)

## The Intellectual Property Rights on all work undertaken under this contract, including the project reports and any spreadsheets developed will be in line with the contracts standard terms and conditions

# payment

## Prices should be submitted in pounds sterling and be inclusive of expenses and exclusive of VAT.

## The Authority require invoices to be submitted within one month of the end of the project.

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## The Authority shall pay the Potential Provider within Thirty (30) calendar days of receipt of a valid invoice, paid against a valid Purchase Order issued by the Authority; the method of payment will be by BACS.

# additional information

## Not Applicable.

# Location

## The location of the Services will be carried out at the Potential Provider’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.