Navy Commercial

4 Deck

Navy Command Headquarters

Leach Building

Whale Island

Portsmouth

PO2 8BY

Telephone: 03001554129

Email: eliot.murton100@mod.gov.uk

13 October 2023

Dear Sir / Madam

**Invitation to Tender Reference** **708926451**

1. You are invited to tender for the ICT Engineering Management and In-Service Support in a further competition under Crown Commercial Services framework RM6100 Lot 3B.

2. The requirement is set out in the Statement of Requirements/Specification. Tenders will be evaluated in accordance with the Tender Evaluation Criteria.

3. The resulting contract will be based on the framework Terms & Conditions. As this is not a negotiated procurement, the Terms & Conditions cannot be amended following contract award.

4. The total budget is £4,300,000.00 (excluding VAT).

5. You may raise questions about the tender and the requirement via the CCS eSourcing Suite. The deadline for asking questions is 10:00 on 20 October 2023. Please note that any questions raised, and the answers provided, may be shared with other interested suppliers.

6. Your tender must be submitted electronically via the CCS eSourcing Suite no later than 10:00 on 30 October 2023. You should allow sufficient time for submission as late tenders will not be accepted. A Tenderers Response Form should be completed to provide answers to all evaluation questions, include all completed documents and provide all requested prices. Any questions about the Terms & Conditions must be raised during this period, as the terms cannot be amended following contract award.

7. The anticipated date for the contract award decision is 6 November 2023. Please note that this is an indicative date and may change.

Yours faithfully

Eliot Murton

Commercial Manager

**Contents**

This invitation consists of the following documentation:

* Invitation to Tender:

1. Glossary

2. Introduction

3. Terms of Participation

4. Further Competition Timetable

5. Completing and Submitting a Tender

6. Questions and Clarifications

7. Tender Evaluation Summary

8. Commercial Evaluation Criteria

9. Financial Evaluation Criteria

10. Technical Evaluation Criteria

11. Award Decision

12. Other Information

* Tenderers Response Form
* Draft Framework Call Off Order Form
* Framework Call Off Terms & Conditions and Schedules (per CCS webpage)
* Cyber Risk Assessment

1. **Glossary**

|  |  |
| --- | --- |
| Agent | means Crown Commercial Service |
| Authority or Contracting Authority | means the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland, (referred to in this document as "the Authority"), acting as part of the Crown – also known as Ministry of Defence |
| Contract | means the contractually-binding terms and conditions set out in this ITT to be entered into between the Authority and the successful Tenderer at the conclusion of this Procurement; |
| eSourcing Suite | means the online tender management and administration system used by the Authority; |
| Evaluation Score | means the score achieved by a Tender at the conclusion of the Evaluation process; |
| Regulations | means the Public Contracts Regulations 2015 (<http://www.legislation.gov.uk/uksi/2015/102/contents/made> |
| Services | means the deliverables (goods and/or services) that may be provided by Suppliers, as set out in the Statement of Requirements/Specification; |
| Technical Evaluation | means the qualitative evaluation of a Tender undertaken during the Evaluation process; |
| Technical Score | means the score awarded to a Tenderer at the conclusion of the Technical Evaluation process; |
| Tender or Bid | means the Tenderer’s formal offer in response to the Invitation to Tender; |
| Tender Submission Deadline | means the time and date set for the latest uploading of Tenders. |
| Tenderer or Supplier | means a framework supplier submitting a proposal to this Procurement; |
| You or Your | means mean the tenderers organisation, or the organisation the tenderers represent |
| We, Us or Ours | means the Authority or Ministry of Defence |

1. **Introduction**
   1. This Procurement will establish a contract for the purchase of Services described in the Statement of Requirements/Specification.
   2. The resulting Contract will be for 3 years.
   3. The maximum contract value is £4,300,000.00.
   4. This resulting Contract will be between the successful Supplier and the Authority. This is a call off contract and as such the Authority cannot guarantee volumes of work.
   5. This tender is being conducted under the Crown Commercial Service Operational Services – Operational Management Framework Agreement (reference RM6100 - Lot 3B) and it’s Terms and Conditions will govern any resultant Contract.
   6. Only those suppliers on the stated framework and lot can submit a tender in response to this requirement.
   7. The Authority is managing this Procurement in accordance with the Public Contracts Regulations 2015.

1. **Terms of Participation**
   1. You must comply with the rules in this Bid Pack and any other instructions given by us. You must also ensure members of your consortium (if relevant), group companies, subcontractors or advisers comply.
   2. You may Submit one bid.
   3. Your bid must remain valid for 90 days after the bid submission deadline.
   4. You must submit your bid in English and through the eSourcing Suite only.
   5. You are able to bid with named subcontractors to deliver parts of the requirements. You must tell us about any changes to subcontractors or you may be excluded from this competition.
   6. We may make enquiries. For example, where you either submit a bid:

* In your own name and or as a subcontractor and or as a member of a consortium connected with a separate bid.
* In your own name which is similar to a separate bid from another bidder within your group of companies.

This is so we can be sure that your involvement doesn’t cause:

* Potential or actual conflicts of interest.
* Supplier capacity problems.
* Restrictions or distortions in competition.
  1. We may require you to amend or withdraw all or part of your bid if, in our reasonable opinion, any of the above issues have arisen or may arise.
  2. Only you or, as applicable, your subcontractors (as set out in your bid) or consortium members (if relevant) can provide services through the contract.
  3. You must not attempt to influence the contract award process. For example, you must not ever directly or indirectly:
* Collude with others over the content and submission of bids. However, you may work in good faith with a proposed partner, supplier, consortium member (if relevant) or provider of finance.
* Canvass our staff or advisors about this competition.
* Try to get information from any of our and/or Contracting Authority staff or advisors about another bidder or bid.
  1. You must ensure that no conflicts of interest exist between you and us / Contracting Authority. If you do not tell us about a known conflict, we may exclude you from the competition. We may also exclude you if a conflict cannot be dealt with in any other way.
  2. You must keep the contents of this Bid Pack confidential (including the fact that you have received it). This obligation does not apply to anything you have to do to submit a bid or comply with a legal obligation.
  3. You must not publicise the deliverables or the award of any contract unless the Contracting Authority has given written consent. For example, you are not allowed to make statements to the media about any bid or its contents.
  4. We reserve the right to:
* Waive or change the requirements of this Bid Pack without notice.
* Verify information, seek clarification or require evidence or further information about your bid
* Withdraw this Bid Pack at any time, or re-invite bids on the same or alternative basis.
* Choose not to award any contract or Lot as a result of the competition.
* Choose to award different Lots at different times.
* Make any changes to the timetable, structure or content of the competition.
  1. We reserve the right to exclude you if:
* You submit a non-compliant bid.
* Your bid contains false or misleading information.
* You fail to tell us of any change in the contracting arrangements between bid submission and award.
* You fix or adjust any element of the Tender by agreement or arrangement with any other person.
* The change in the contracting arrangements would result in a breach of procurement law.
* For any other reason provided in this Bid Pack.
* For any reason set out in the Public Contracts Regulations 2015.
  1. If a misrepresentation by you induces the Contracting Authority to enter into a contract with you, you may be excluded from bidding for contracts for three years, under regulation 57(8)(h)(i) of the PCR 2015 or sued by the Contracting Authority for damages, the Contracting Authority may rescind the contract under the Misrepresentation Act 1967.
  2. If fraud, or fraudulent intent, can be proved, you may be prosecuted and convicted of the offence of fraud by false representation under s.2 of the Fraud Act 2006, which can carry a sentence of up to 10 years or a fine (or both).
  3. If there is a conviction, then your organisation must be excluded from procurement for five years under reg. 57(1) of the PCR 2015 (subject to self-cleaning).
  4. We will not pay your bid costs for any reason.
  5. The Contracting Authority will not be liable:
* Where parts of the Bid Pack are not accurate, adequate or complete.
* For any written or verbal communications.
  1. You must carry out your own due diligence and rely on your own enquiries.
  2. This Bid Pack is not a commitment by the Contracting Authority to enter into a contract.
  3. The Bid Pack remains our property. You must use the Bid Pack only for this competition.
  4. You allow us to copy, amend and reproduce your bid so we can:
* Run the competition.
* Comply with law and guidance.
* Carry out our business.
  1. Our advisors, subcontractors and other government bodies can use your bid for the same purposes.
  2. We will not share any information from your bid which you have identified as being confidential or commercially sensitive with third parties, other than stakeholders in the competition. We may however share this information, but only in line with the Regulations, the Freedom of Information Act 2000 (FOIA) or any other law as applicable.

1. **Further Competition Timetable**
   1. The timetable below are intended timelines but, for a range of reasons, dates can change. We will tell you if and when timelines change.

|  |  |  |  |
| --- | --- | --- | --- |
| **Stage** | **Date and Time** | **Responsibility** | **Submit to:** |
| Final date for  Clarification Questions | 20 October 2023 | Tenderers | CCS eSourcing Suite |
| Final Date for Requests for Extension to return date | 20 October 2023 | Tenderers | CCS eSourcing Suite |
| Authority issues Final Clarification Answers | 24 October 2023 | Authority | All Tenderers |
| Tender Return | 30 October 2023 | Tenderers | CCS eSourcing Suite |
| Tender Evaluation Commences | 30 October 2023 | Authority | N/A |

1. **Completing and Submitting a Tender**
   1. To participate in this competitive tendering exercise, Tenderers are required to submit a Tender which fully complies with the instructions in this Bid Pack.
   2. Your bid must be made by the organisation that will be responsible for providing the deliverables if your bid is successful.
   3. You must enter your bid into the e-Sourcing Suite. Only bids received through the e-Sourcing Suite will be accepted.
   4. Make sure you answer every question. Each question must be answered in its own right. You must not answer any of the questions by cross referencing other questions or other materials e.g. reports located on your website.
   5. Tenderers are strongly advised to read through all documentation first to ensure they understand how to submit a fully compliant Tender.
   6. It is the Tenderer’s responsibility to ensure that a fully compliant Tender is submitted.
   7. Tenderers must ensure that they are using the latest versions of this document, as the documentation may be updated from time to time.
   8. For technical guidance on how to complete questions and text fields, and how to upload any requested attachments please see CCS Supplier Guidance <https://crowncommercialservice.bravosolution.co.uk/web/login.html>
   9. Should any exclusions, assumptions, dependencies or caveats apply to your Tender or any of the goods and/or services that you would provide when delivering the requirements, these should be clearly indicated in the relevant areas of the Tender.

* 1. Submit your bid before the Bid Submission Deadline.
  2. Press the Submit Response button when your bid is ready, otherwise we will not be able to see it.

1. **Questions and Clarifications**
   1. If you have any questions you need to ask them as soon as possible after the procurement event is published as there is a deadline for submitting clarifications questions. This gives you the chance to check that you understand everything before you submit your bid.
   2. You need to send your questions through the eSourcing Suite. This is the only way we can communicate with bidders. Ensure your question is specific and clear and does not include your identity. This is because we publish all the questions and our responses to all bidders.
   3. If you feel that a particular question should not be published, you must tell us why when you ask the question. We will decide whether or not to publish the question and response.
   4. You can ask us questions about the competition but please do not attempt to ‘negotiate’ the terms. All contract awards will be subject to the terms and conditions identified in this Tender.
   5. The Authority reserves the right to contact Tenderers at any time for clarification on all or any part of their Tender during this Procurement and which is likely to require a prompt response.
2. **Tender Evaluation Summary**
   1. The Tender evaluation will assess the Most Economically Advantageous Tender (MEAT) to The Authority based on the following calculation:

Highest Total Evaluation Score from the following evaluation elements:

Commercial Qualification – Pass/Fail only and not included in the total Evaluation Score.

Financial Price Score – Worth 20% of the total Evaluation Score.

Technical Quality Score – Worth 80% of the total Evaluation Score.

* 1. The Technical Score will be added to the Financial Score to determine the “Evaluation Score” for each Tenderer. This will be calculated on a Technical/Financial split of 80%/20%.

*Example calculation, for information purposes only and based on financial score worth 50% and Technical score worth 50% - figures for this procurement may differ.*

*In this example, Tenderer B has the highest total evaluation score and is the winning tenderer.*

|  |  |  |  |
| --- | --- | --- | --- |
| *Tenderer* | *Technical Score*  *(maximum 50)* | *Financial Score*  *(maximum 50)* | *Evaluation Score*  *(maximum 100)* |
| *Tenderer A* | *35* | *50* | *85* |
| *Tenderer B* | *45* | *45* | *90* |
| *Tenderer C* | *40* | *25* | *65* |

* 1. Any Tender which is considered non-compliant for any Commercial, Financial or Technical element or criteria will be excluded from the competition and not receive an Evaluation Score. If a tender is considered non-compliant in either the Commercial or Financial evaluations that tender may be excluded from the Technical evaluations and not receive any Technical scores or feedback.
  2. Scores will be rounded to two decimal places.
  3. In the event that multiple Tenderers achieve the exact same highest Evaluation Score, then the Tenderer with the lowest Total Price will be considered to be the Winning Tenderer. In the event that multiple Tenderers achieve the exact same highest Evaluation Score and have the exact same lowest Total Price, then The Authority reserves the right to request those, and only those, Tenderers to submit final and best Total Prices, with the lowest final and best Total Price considered to be the Winning Tenderer.
  4. Tenderers must provide relevant answers and all requested documentation in response to all commercial qualification, financial and technical criteria/questions. Responses should remain as concise as possible and any supporting information should be relevant to the response.
  5. Tenders will be evaluated based on the contents of their Tender response only. Tenderers should submit only one priced proposal. Technical Evaluation will be undertaken independently from Commercial and Financial Evaluations. Technical evaluators will have no knowledge of associated prices. Tenderers should ensure that there are no prices shown within any responses to, or supporting documents for, for technical criteria.

1. **Commercial Qualification Evaluation Criteria**
   1. The Commercial Qualification Evaluation will assess if all tendering and contractual requirements have been provided.
   2. A Tender will be considered non-compliant if:

* the Tender was not received by the due date and time.
* the full set of requirements cannot be delivered.
* any required delivery dates cannot be met.
* all Framework Terms & Conditions and have not been accepted.
* all required MOD Terms & Conditions and have not been accepted.
* any other required documentation was not submitted.
* any prices have been included in the technical responses and this is considered to have affected the evaluation process.
* the Social Value Commitments form does not include at least one commitment for each of the three Social Value criteria/themes.
  1. The Authority reserves the right to undertake due diligence checks and/or financial health checks of Tenderers as part of the Commercial Evaluation. If any of these checks raises concerns around the Tenderer or If a Parent Company or Bank guarantee is requested and is not provided, The Authority will consider the Tenderer non-compliant. If these checks are undertaken on the Winning Supplier during the standstill period prior to formal contract award, the Authority reserves the right to award the Contract to the next best placed Supplier or to cancel or re-run the procurement.

1. **Financial Price Evaluation Criteria**
   1. Tenderers are required to complete the Pricing Table.
   2. The Financial Evaluation will assess the Total Price the Tenderer has offered to deliver all the requirements set out in the Statement of Requirements/Specification.
   3. As the maximum duration for this contract is longer than 3 years, Variation of Price (VOP) will apply to prices for any goods and/or services delivered after 3 years. Any prices stated for the Contract Periods must be the same as the prices for Contract Period 1. Any VOP calculation will be made as necessary during the contract term.
   4. Prices should be provided for each item listed in the Pricing Table. This shall be the total maximum cost for the provision of all goods and/or services listed, as detailed in the Statement of Requirement, for the quantities quoted and for the full maximum duration of the requirement, including any optional goods/services and/or periods. All prices submitted must be excluding VAT.
   5. The Total Price figure that will be used in the evaluation of Tenders shall be the total figure that is calculated from the prices Tenderers have provided for each item listed in the Pricing Table, for the full maximum duration of the requirement, including any optional goods/services and periods.
   6. Tenderers are notified that when the contract is in place, payments for goods and/or services will be made after the goods and/or services have been fully delivered. For example, payment for purchase of an item will be made after it has been delivered and installed or payment for annual maintenance of a piece of equipment will be made at the end of the contract year during which the maintenance was undertaken.
   7. Where estimated Authority usage figures are shown on the Schedule of Requirements, the Total Price figure shall not be a guarantee of quantities required or payments to be made under any resulting Contract. The quantity of each item is for evaluation purposes only and, whilst this may give an indication of numbers or proportions of each type of goods and/or services that may be required, quantities required under the contract may be higher or lower based on Authority requirements during the contract period. The contract value will be a limit of liability under which the Authority shall be entitled to purchase the goods and/or services listed at the firm prices set.
   8. A Tender will be considered non-compliant if:

* the Total Price is greater than the total available funding of £4,300,000.
* Annex A shows an incorrect Total Price as the Total Price calculation is above the available funding.
* the Tender does not indicate a Total Price.
* the Tender has not provided prices for all items in the Schedule of Requirements/Pricing Table.
* the Tender requires the Authority to provide additional resource (other than any identified in the Statement of Requirements), therefore the pricing does not cover all requirements.
  1. The Tenderer with the lowest total price (provided the tender is fully compliant) shall be awarded the maximum Financial Score available. The remaining Tenderers shall be awarded a percentage of the maximum Financial Score available, based on their price relative to the lowest price submitted.
  2. The calculation used is the following:

Lowest Price from a compliant Tender x maximum Financial Score available

Tenderers price

*Example calculation, for information purposes only and based on maximum Financial score of 50% and Technical score of 50% - figures for this procurement may differ.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Tenderer*** | ***Price Submitted*** | ***Score Calculation*** | ***Maximum Score Available*** | ***Financial Score Awarded*** |
| *Tenderer A* | *£1,000* | *(£1,000 / £1,000) x 50* | *50* | *50* |
| *Tenderer B* | *£1,100* | *(£1,000 / £1,100) x 50* | *50* | *45* |
| *Tenderer C* | *£2,000* | *(£1,000 / £2,000) x 50* | *50* | *25* |

1. **Technical Quality Evaluation Criteria**
   1. The Technical Evaluation will assess the Tender response to establish the level of confidence The Authority has that the Tenderer will be able meet and deliver all the requirements detailed in the Statement of Requirements/Specification.
   2. The response to each criteria will be given points in accordance with the table below:

Criteria 1 to 13 will be scored in accordance with the following:

|  |  |  |  |
| --- | --- | --- | --- |
| 100 – High Confidence  In The Authority’s opinion the Tenderers response to the requirements or criteria being assessed: | 70 – Good Confidence  In The Authority’s opinion the Tenderers response to the requirements or criteria being assessed: | 30 – Moderate Confidence  In The Authority’s opinion the Tenderers response to the requirements or criteria being assessed: | 0 – Low Confidence  In The Authority’s opinion the Tenderers response to the requirements or criteria being assessed: |
| addresses and demonstrates a thorough understanding of all elements of the requirement or criteria, where applicable. | addresses and demonstrates a sufficient understanding of most of the requirement or criteria, where applicable. | addresses and demonstrates an understanding of some of the elements of the requirement or criteria, where applicable. | does not address or demonstrate an understanding of most or all of the requirement or criteria, where applicable. |
| provides a comprehensive, unambiguous and thorough explanation of how all of the requirement or criteria will be delivered, where applicable. | provides sufficient detail and explanation of how most of the requirement or criteria will be delivered, where applicable. | is weak in some areas and does not fully detail or explain how some elements of the requirement or criteria will be delivered, where applicable. | does not demonstrate the ability to deliver most or all of the requirement or criteria, where applicable. |
| details a thorough explanation of how the full volumes and timescales of the requirement or criteria will be met, where applicable. | shows sufficient ability to meet most of the volumes and timescales for the requirement or criteria, where applicable. | indicates that some of the volumes or timescales for the requirement or criteria will be met but may be lacking detail is some areas, where applicable. | does not show that most or all of the volumes or timescales of the requirement or criteria will be met, where applicable. |
| provides comprehensive details showing how all of the requirement or criteria will be managed with sufficient resource allocated and support provided for the full duration, where applicable. | provides sufficient information to show how most of the requirement or criteria will be managed with adequate resource allocated and support provided, where applicable. | provides details of how some of the requirement or criteria will be managed but leaves concerns about the resource and support provided, where applicable.  . | does not provide details of how most or all of the requirement or criteria will be managed or that the required resource and support will be provided, where applicable. |
| comprehensively details how the requirement or criteria will be assured and how all quality or standards expected will be met in full, where applicable. | sufficiently details how most of the requirement or criteria will be assured and quality or standards expected will be met, where applicable. | provides details of how some of the requirement or criteria will be assured but leaves doubt about quality or standards, where applicable. | does not demonstrate that most or all of the required standards or quality will be met, where applicable. |
| has comprehensively considered risks to delivery of the requirement or criteria and thoroughly explained how they will be eliminated or mitigated, where applicable. | has considered risks to delivery of the requirement or criteria and adequately indicated how most will be eliminated or mitigated, where applicable. | has considered risks to some of the requirement or criteria but leaves concerns that there are risks that have not been considered or may not be mitigated, where applicable. | has identified and addressed few or no risks to delivery, where applicable. |

* 1. The points achieved will be multiplied by the corresponding weighting to provide an overall criteria mark.
  2. When the mark for each question has been determined they will be added together to provide a total mark for the Technical Evaluation.
  3. The evaluators are considered to be Subject Matter Experts (SME) on the Statement of Requirements/Specification. If an individual criteria is evaluated by more than the one SME, The Authority will review the points allocated by the individual evaluators before facilitating a group consensus meeting. During the meeting, evaluators will discuss their independent points until they reach a consensus regarding the points that should be attributed to each Tenderers answer to the questions.
  4. Evaluators will assess each question individually and will not be expected to search for answers. Where a Tenderers answer to any technical criteria question is covered within a separately attached document, the text answer to that criteria question must clearly indicate the relevant part of the supporting document in which the answer can be found. Any documents that have not been referenced will be discounted during evaluation.
  5. Once all technical responses have been evaluated the individual marks attributed to each response, excluding any pass/fail criteria, will be added together to provide a total Technical Mark.
  6. A Tender will be considered non-compliant if:
* the Tender receives a fail on any pass/fail criteria.
* the Tenderer has self-certified that that they cannot meet any of individual pass/fail criteria.
* the Tender receives points which are below the threshold set for any individual criteria.
* the Tender receives a score of 0 on more than one of the three social value MAC criteria.
  1. Tenderers ‘Technical Score’ shall be calculated as a percentage of the maximum Technical Score available, based of the total Technical Marks received.

The calculation used is the following:

Tenderers Total Marks x maximum Technical Score available

Total Marks Available

*Example calculation, for information purposes only and based on maximum Financial score of 50% and Technical score of 50% - figures for this procurement may differ.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Tenderer*** | ***Total Marks*** | ***Score Calculation*** | ***Maximum Score Available*** | ***Technical Score Awarded*** |
| *Tenderer A* | *70* | *(70 / 100) x 50* | *50* | *35* |
| *Tenderer B* | *90* | *(90 / 100) x 50* | *50* | *45* |
| *Tenderer C* | *80* | *(80 / 100) x 50* | *50* | *40* |

* 1. The Technical evaluation questions/criteria that Tenderers should address within their Tender are:

| **Figure** | **Criteria** | **Points Available** | **Minimum Threshold** | **Weight** | **Mark Available** | **Word Count** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Explain your approach and Method - how the solution meets our requirement. | 0, 30, 70 or 100 | 30 | 5% | 10 | 150 |
| 2 | Explain your service structure and how it will meet the service level requirements and deliver the relevant skills and experience. | 0, 30, 70 or 100 | 30 | 10% | 10 | 150 |
| 3 | Demonstrate experience delivering the service requirements described in Output 1 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 4 | Demonstrate experience delivering the service requirements described in Output 2 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 5 | Demonstrate experience delivering the service requirements described in Output 3 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 6 | Demonstrate experience delivering the service requirements described in Output 4 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 7 | Demonstrate experience delivering the service requirements described in Output 5 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 8 | Demonstrate experience delivering the service requirements described in Output 6 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 9 | Demonstrate experience delivering the service requirements described in Output 7 | 0, 30, 70 or 100 | 70 | 10% | 15 | 400 |
| 10 | Explain your how your service represents value for money. | 0, 30, 70 or 100 | 30 | 5% | 10 | 150 |
| 11 | MAC3.1 - Explain how you will Create a diverse supply chain to deliver the contract including new businesses and entrepreneurs, start-ups, SMEs, VCSEs and mutuals. | 0, 30, 70 or 100 | 30 | 2.5% | 2.5 | 100 |
| 12 | MAC4.2 - Explain how you will Influence staff, suppliers, customers and communities through the delivery of the contract to support environmental protection and improvement. | 0, 30, 70 or 100 | 30 | 5% | 5 | 150 |
| 13 | MAC6.1 - Explain how you will demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce. | 0, 30, 70 or 100 | 30 | 2.5% | 2.5 | 100 |
|  |  |  |  | 100% | 100 | 2400 |

* 1. Social Value Overview (for criteria 11-13)

Social value has a lasting impact on individuals, communities, and the environment. Government has a huge opportunity and responsibility to maximise benefits effectively and comprehensively through its commercial activity. It cannot afford not to. A missed opportunity to deliver social value may lead to costs that the taxpayer has to absorb elsewhere through public procurement.

A competitive and diverse supply landscape can help to deliver innovation in public services, manage risk and provide greater value for taxpayers’ money.

As a result, the Social Value Model (SVM) has been created which details 5 Themes, 8 Policy Outcomes and 24 Model Award Criteria (MACs). The SVM MACs are questions which relate to Social Value. The use of the SVM is mandatory in all central government procurements using Public Contracts Regulations (PCR) 2015 and Defence and Security Public Contracts Regulations (DSPCR) 2011 above financial threshold and exempt procurements.

Defence is focusing on three, out of the five, priority Social Value themes that are most relevant for Defence:

* Tackling economic inequality.
* Fighting climate change; and
* Equal opportunity.

The Social Value Scoring Criteria is listed below. Please use this and the information provided within the SVM to compile your responses to the SVM MAC and Model Evaluation Question (MEQ) asked. In compiling your answer, please refer to the SVM Quick Reference Table. Under Model Response Guidance for tenderers and evaluators examples of types of evidence the tender evaluators are looking for can be found.

Alongside the Example Reporting Metrics, Social Value Key Performance Indicators (KPIs) may be used within this contract. KPIs will be generated from the Tenderer’s social value response it is therefore important that measurable commits are included in the response (both commitments against the reporting metrics and other metrics as may be appropriate. KPIs may be agreed between the parties and included in the contract at Contract Award.

The aim of the following SVM MACs is to understand the Tenderers Social Value Commitment that this procurement programme will provide within the geographical location(s) that is will be delivered from.

In your written response you should provide convincing arguments, including suitable evidence, of What your understanding of Social Value is, in relation to this procurement, and How you will instil confidence in the Authority in your ability to deliver against the Social Value requirements for this procurement.

A list of some of the key response documents that the Authority would expect you to provide are provided below. However, within the overall limit of pages you should supplement your written submission with other documents you consider will build confidence in your ability to maximise Social Value Commitments.

From the information that you provide, the evaluators will assess, qualitatively, your response, based on the information that you provide within your tender response.

Alongside their Commitments against the reporting metrics, the successful Tenderer’s method statement will form the basis of Key Performance Indicators and jointly managed throughout the life of the contract.

The Tenderers must ensure that they answer the SVM MACs asked. Any additional information which is not specific to the contract being procured will not be considered.

The Tenderers responses are to set out the additional Social Value benefits that they will deliver against the Policy Outcomes for this procurement. It is not sufficient to only reference/use to their Corporate Social Responsibility (CSR) and or Environmental, Social and Governance (ESG) documents.

Within the maximum word count, describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria. Please include:

* your ‘Method Statement,’ stating how you will achieve this and how your commitment meets the SVM Model Award Criteria (MAC), and
* a timed project plan and process, including how you will implement your commitment and by when
* how you will monitor, measure and report on your commitments/the impact of your proposals. You should include but not be limited to:

· timed action plan

· use of metrics

· tools/processes used to gather data

· reporting

· feedback and improvement

· transparency

* how you will influence your: staff, supply chains, 3rd party suppliers, customers, and communities through the delivery of the contract to support the Policy Outcome, e.g., engagement, co-design/creation, training, and education, partnering/collaborating, volunteering.

In complying your answer, please refer to the Social Value Model Quick Reference Table, under Model Response Guidance for tenderers and evaluators for examples of types of evidence the tender evaluators are looking for: The written submission should be in 11pt Arial to meet the response requirement.

For this procurement, the following SVM MAC have been selected as being appropriate.

|  |  |  |
| --- | --- | --- |
| **Model Award Criteria** | **Model Response Guidance for tenderers and evaluators**  *The award criteria (left) and sub-criteria (below) will be used to evaluate the response* | **Example Reporting Metrics**  *(proposals to be included in tender response)* |
| **Theme 2: Tackling economic inequality: Policy Outcome: Increase supply chain resilience and capacity** | | |
| MAC 3.1: Create a diverse supply chain to deliver the contract including new businesses and entrepreneurs, start-ups, SMEs, VCSEs and mutuals. | Activities that demonstrate and describe the tenderer’s existing or planned:  ● Understanding of the types of businesses in the market and the level of participation by new businesses, entrepreneurs, start-ups, SMEs, VCSEs and mutuals.  ● Activities to identify opportunities to open sub-contracting under the contract to a diverse range of businesses, including new businesses, entrepreneurs, start-ups, SMEs, VCSEs and mutuals.  ● Plans for engaging a diverse range of businesses in engagement activities prior to appointing supply chain members (including activities prior to award of the main contract and during the contract term).  ● Activities that demonstrate a collaborative way to work with a diverse range of businesses as part of the supply chain.  Illustrative examples: co-design and co-creation of services; collaborative performance management; appropriate commercial arrangements; inclusive working methods; and use of inclusive technology.  ● Advertising of supply chain opportunities openly and to ensure they are accessible to a diverse range of businesses, including advertising sub-contracting opportunities on Contracts Finder.  ● Ensuring accessibility for disabled business owners and employees.  ● Structuring of the supply chain selection process in a way that ensures fairness (e.g. anti-corruption) and encourages participation by a diverse range of businesses, including with regard to new businesses, entrepreneurs, start-ups, SMEs, VCSEs and mutuals. | For each of start-ups, SMEs, VCSEs, mutuals  ■ The number of contract opportunities awarded under the contract, and value.  ■ Total spend under the contract, as a percentage of the overall contract spend.  Number/Percentage of supply chain opportunities advertised in an accessible media |
| **Theme 3: Fighting Climate Change: Policy Outcome: Effective stewardship of the environment** | | |
| MAC 4.2 Influence staff, suppliers, customers and communities through the delivery of the contract to support environmental protection and improvement. | Activities that demonstrate and describe the tenderer’s existing or planned:  ● Understanding of how to influence staff, suppliers, customers, communities and/or any other appropriate stakeholders through the delivery of the contract to support environmental protection and improvement.  ● Activities to reconnect people with the environment and increase awareness of ways to protect and enhance it.  Illustrative examples:   * Engagement to raise awareness of the benefits of the environmental opportunities identified. ○ Co-design/creation. Working collaboratively to devise and deliver solutions to support environmental objectives. * Training and education. Influencing behaviour to reduce waste and use resources more efficiently in the performance of the contract. * Partnering/collaborating in engaging with the community in relation to the performance of the contract, to support environmental objectives. * Volunteering opportunities for the contract workforce, e.g. undertaking activities that encourage direct positive impact. | Number of people-hours spent protecting and improving the environment under the contract. |
| **Theme 4: Equal opportunity: Policy Outcome: Tackle workforce inequality** | | |
| MAC 6.1 Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce | Activities that demonstrate and describe the tenderer’s existing or planned:  ● Understanding of the issues affecting inequality in employment, skills and pay in the market, industry or sector relevant to the contract, and in the tenderer’s own organisation and those of its key sub-contractors.  ● Measures to tackle inequality in employment, skills and pay in the contract workforce. Illustrative examples:   * Inclusive and accessible recruitment practices, and retention-focussed activities. * Offering a range of quality opportunities with routes of progression if appropriate, e.g. T Level industry placements, students supported into higher level apprenticeships. * Working conditions which promote an inclusive working environment and promote retention and progression. * Demonstrating how working conditions promote an inclusive working environment and promote retention and progression. * A time-bound action plan informed by monitoring to ensure employers have a workforce that proportionately reflects the diversity of the communities in which they operate, at every level. * Including multiple women, or others with protected characteristics, in shortlists for recruitment and promotions. * Using skill-based assessment tasks in recruitment. * Using structured interviews for recruitment and promotions. * Introducing transparency to promotion, pay and reward processes. * Positive action schemes in place to address under-representation in certain pay grades. * Jobs at all levels open to flexible working from day one for all workers. * Collection and publication of retention rates, e.g. for pregnant women and new mothers, or for others with protected characteristics. * Regular equal pay audits conducted | Total number/percentage of full-time equivalent (FTE) people from groups under-represented in the workforce employed under the contract, as a proportion of the total FTE contract workforce    Total number/percentage of people from groups under-represented in the workforce on apprenticeship schemes / other training schemes under the contract, as a proportion of the all people on apprenticeship schemes/ other training schemes within the contract workforce |

Further Social Value Guidance can be found:

a) Social Value Model (SVM), Government Commercial Function, Edition 1.1 – 3 Dec 20 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940827/Guide-to-using-the-Social-Value-Model-Edn-1.1-3-Dec-20.pdf>

b) Guide to Using the Social Value Model, Government Commercial Function, Edition 1.1 – 3 Dec 20 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940826/Social-Value-Model-Edn-1.1-3-Dec-20.pdf>

c) Social Value Model Quick Reference Table, Government Commercial Function, Edition 1.1 – 3 Dec 20 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940828/Social-Value-Model-Quick-Reference-Table-Edn-1.1-3-Dec-20.pdf>

1. **Award Decision**
   1. Following evaluation of Tenders in accordance with the evaluation process set out in this ITT, the Tenderer which offers the most economically advantageous Tender may be awarded a Contract.
   2. The Tender which receives the highest Evaluation Score, which is calculated as the highest combined Technical Evaluation Score and Financial Evaluation Score (provided the tender is considered fully compliant in all evaluation areas) shall be considered the most economically advantageous Tender.

1. **Other Information**

12.1 Save as set out in PPN 01/22, the Authority will not be accepting Tenders that:

a. contain any Russian/Belarussian products and / or services; and/or

b. are linked to entities who are constituted or organised under the law of Russia or Belarus, or under the control (full or partial) of a Russian/Belarusian person or entity. Please note that this does not include companies:

(1) registered in the UK or in a country with which the UK has a relevant international agreement with reciprocal rights of access in the relevant field of public procurement; and / or

(2) which have significant business operations in the UK or in a country the UK has a relevant international agreement with reciprocal rights of access in the relevant field of public procurement.

Tenderers must confirm in writing that their Tender, including any element that may be provided by any part of the Contractor’s supply chain, does not contain any Russian/Belarusian products and/or services.

Tenderers must include provisions equivalent to those set out in this clause in all relevant Sub-Contracting Arrangements.

**Contract Documents**

Any contract resulting from this tender will be formed from the CCS Framework Order Form, Terms & Conditions and associated Schedules, including the Statement of Requirements/Specification and Pricing Table, incorporating prices submitted by the Winning Tenderer.

If, following the contract award decision, the Winning Tenderer does not agree to the Contract terms (when the Contract has been drafted in accordance with the terms and information provided in this tender), the Authority reserves the right to terminate that contract award decision and award the Contract to the next best placed Tenderer or to cancel or re-run the procurement.

If the Winning Tenderer enters into the contract but is unable to deliver the requirements, the Authority reserves the right to terminate that Contract and award the Contract to the next best placed Tenderer or to cancel or re-run the procurement.

**IR35**

IR35 off payroll working rules are not expected to apply to this requirement unless the Winning Tenderer indicates that the personnel who will be used to deliver Services will not be employed through their payroll. In those circumstances, a relevant assessment will be considered.

**Cyber Risk**

A Cyber Risk Assessment has been raised and the profile is Low. The reference is RAR-866613319.

A Supplier Assurance Questionnaire does need to be completed.

Where a Supplier Assurance Questionnaire needs to be completed, Tenderers must complete and email this to [ISSDes-DCPP@mod.gov.uk](mailto:ISSDes-DCPP@mod.gov.uk) who will confirm cyber risk compliance. A copy of the completed questionnaire and the compliance email should then be included as part of the tender submission.

If a Tenderers Supplier Assurance Questionnaire score does not meet the level set in the Cyber Risk Assessment, this does not prevent submission of a Tender. In those circumstances, a Cyber Implementation Plan should be completed as part of the tender submission, to demonstrate what actions will be taken to meet the required Cyber Risk level. Provided the actions and timescales were considered acceptable to The Authority, the Cyber Implementation Plan would then be included as a requirement in any resulting Contract.

Guidance of Cyber Implementations Plans can be found online at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1126692/20221219-CIP_Guidance.pdf>

**Cyber Implementation Plan Template**

|  |  |
| --- | --- |
| MOD contract number: |  |
| CSM Risk Acceptance Reference: |  |
| CSM Cyber Risk Profile: |  |
| Name of Supplier: |  |
| Current level of Supplier compliance: |  |
| Reasons unable to achieve full compliance: |  |
| Measures planned to achieve compliance / mitigate the risk with dates: |  |
| Anticipated date of compliance / mitigations in place: |  |

**Statement of Requirements/Specification**

**Introduction**

1. Navy Command (NC), Maritime C5ISR Support Unit (MCSU) requires **Engineering Management, Portfolio Management and In-Service Support** for all non-Enterprise Information and Communications Technologies (ICT) used across the Royal Navy (RN) Estate.
2. This non-Enterprise ICT empowers the full range of NC Outputs and Activities, from CASD, Operational Deployments, Ops support, through to Non-Operational day-to-day business as usual. These ICT systems and equipment sets are used across the entire range of Ships, Submarines, Air Stations, RN flights, RM units, HQs, Naval Bases and RN/RM Shore Establishments/Barracks. There are more than 13,000 equipment/system elements in use, these consist of Computers, Servers, Networks Switches/Routers, Laptops, Tablets, Audio-Visual Equipment, Printers and Cameras.

**Overview of Requirement**

1. The Technical Services required enable the provision of equipment to facilitate RN tasks such as Security, Intelligence Gathering, Navigation, Engineering Support, Personnel Management, Logistics, Budgeting, Safety, Training, etc and in all instances where there is no corporate MOD Business Services, JFC/DD (inc. MoDNET/OpNET) or DE&S solution available.
2. These Technical Services are managed and supported across the RN by this essential end-to-end Engineering, Technical and Project/Portfolio Management Service, which, cover all types of non-Enterprise MOD ICT, that is funded and used solely by NC TLB.
3. Technical Services include Project Management of this ICT portfolio to deliver value for money and coherent Technical Management across NC, to ensure ICT Security Accreditation, Information Assurance/Security and Asset Management to meet JSP 440 Security Regulations and HMG/MOD Information Assurance Policy.
4. The day-to-day management of this service provision is essential to ensure continued RN functionality. Without these services there would be a rapid effect on the ability of the RN to complete a wide range of activities/outputs across NC, impacting the RN’s ability to deliver Operations, Defence standing and contingent tasks. NC HQ would lose all management and control of In-Service ICT Support, Maintenance, Repair and Programme/Portfolio Management.

**SOW Deliverables – Outcome Description**

1. The day-to-day management of all **Engineering Management, Project/Portfolio Management and In-Service Support** for NC supplied equipment and systems, providing the following services:
2. Implementation of all MOD mandated Security Applications/Procedures on NC ICT assets as a managed service.
3. Project manage and deliver ICT Hardware/Software and support solutions to NC end users to agreed timeframes and budget constraints.
4. Asset tracking, to document the current state of ICT throughout NC. This database records all Hardware/Software/Licencing and Configuration elements about assets to include IT security accreditation details, in accordance with the direction provided by HMG, MOD and NC Information Assurance and Security Regulations and policy.
5. Mobile technical support to larger fixed networks and systems installed at NC locations throughout the UK.
6. Build, deliver and support NC ICT equipment and systems supplied to all platforms and establishments, at all security classifications up to and including Above Secret
7. Compilation, Management and delivery of Security Operating instructions (SyOPS), Risk Management and Accreditation Document Sets (RMADS) and other system accreditation documents as part of all NC ICT deliverables, providing this to NC end users in accordance with HMG and MOD IT Security and Information Assurance policy and regulations.
8. Technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions that meet user requirements, compliant with all relevant HMG and MOD policy/regulations, for the provision of ICT in the public sector.
9. Advise on emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative ways of working can be exploited to support NC outputs.
10. ICT Portfolio Project/Programme Management and Through Life Planning and Budgeting for NC ICT.
11. Manage, co-ordinate and deliver all Logistic Support necessary to enable these Technical and Engineering Services, to include Obsolescence Management and disposals.
12. Response to and management of OPDEFs, deploying engineering services globally to support ships/units across the UK and overseas.
13. Management and delivery of ongoing technical upgrades, carrying out this work both in the UK and overseas.
14. Support to a wide range of Navy Digital force generation activity through the enablement of the endorsed Information Exchange Requirement (IER).
15. Enable MCSU to discharge its responsibilities as an ‘Equipment Authority’, ensuring full compliance with Engineering and Safety standards.
16. Manage and deliver ICT and Information Security (INFOSEC) assurance and compliance for all NC delivered operational ICT systems.
17. All the above Technical Services directly enable all current Operations, including critical ongoing support to elements of all Defence Taskings with a maritime contribution.
18. Services are expected to be maintained over the full 36 months duration of the contract , below are the outputs required followed by the activities necessary to fulfil this requirement (details in Annex A):

|  |  |
| --- | --- |
| **Output Reference** | **Description** |
| 1 | ICT Build and Service Management |
| 2 | ICT Programme Management |
| 3 | ICT Logistics |
| 4 | ICT Mobile Device Management & Compliance Engineering |
| 5 | ICT Network and Systems Engineering |
| 6 | ICT Security Support & Compliance Engineering |
| 7 | Navy Command Asset Register Management |

1. The individual Service Outputs they required are described more comprehensively in Annex A – Statement of Technical need, below.

**Timescales**

The Core Requirement of this contract will start on 1st Nov 2023 and run for 36 months at a cost of £4.3M Ex VAT which includes £60K travel and subsistence.

**Location**

Tasking and project work will require attendance, predominantly in and around the Portsmouth Naval Base area, and specifically Portsdown technology Park (PTP), MCSU. The delivery team will be required to visit/work in other Military locations across the UK.

This link, <https://www.royalnavy.mod.uk/our-organisation/bases-and-stations>, shows the main Navy Command managed sites and locations this contract will cover; however, this is not exhaustive as smaller sites may not be listed.

All Travel and Subsistence (T&S) expenses must comply with the MoD T&S Policy.

All suppliers are obliged to provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of GDPR (General Data Protection Regulation) and ensures the protection of the rights of data subjects. For further information please see the Information Commissioner's Office website https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

**Governance**

**Weekly** – Weekly update to the requirement owner on task progress and issues.

**Bi-Annually** – Bi-Annual review with requirement owner to capture Risks and Issues in Microsoft Project Online (under Navy Portfolio) and review progress towards delivery and performance against stated KPIs (Key Performance Indicators) and forward look to set priorities and tasks for the following year.

**Acceptance**

The supplier must conduct an initial onboarding meeting and generate a plan that includes a schedule of works and a resource delivery plan and timeline within 2 weeks of the start of the contract.

**Government Furnished Assets**

Provision of access to the required MoD ICT on which this requirement will be developed and delivered requires a minimum of SC clearance.

**Security**

Security Clearance (SC) is required as a minimum and must be in place at the start of the contract. Some of the outputs listed require a DV in order to deliver, these are listed under each output in Annex A. Suppliers' personnel will be required to visit MOD establishments (e.g. NCHQ, HMNB Portsmouth, Dstl PDW) during the course of the contract and will need to provide evidence of clearances.

**Personal Data**

No personal data will be processed during the course of this contract

**Quality & Standards**

Delivery of the outputs in compliance with the following standards:

*Standards*

|  |  |  |
| --- | --- | --- |
| **Item** | **Number** | **Title** |
| 1 | JSP 604 | Defence Manual for Information and Communications Technology (ICT) |
| 2 | JSP 440 | Defence Manual of Security |
| 3 | JSP 441 | Information, Knowledge, Digital and Data in Defence |
| 4 | JSP 490 | Defence Crypto Security Operating Instructions |
| 5 | JSP 491 | Cryptographic Handling Instructions |
| 6 | JSP 892 | Risk Management |
| 7 | JSP 940 | Quality Management |
| 8 | JSP 945 | MOD Policy for Configuration Management |
| 9 | JSP 375 | Management of Health and Safety in Defence |
| 10 | JSP 418 | Management of Environmental Protection in Defence. |

**Health & Safety**

Work to be conducted in line with MOD H&S practise derived from HSE guidance.

**Environmental**

Work to be conducted in line with MOD Environmental practise.

**Implementation**

The supplier must conduct an initial onboarding meeting and generate a plan that includes a schedule of works and a resource delivery plan and timeline within 2 weeks of the start of the contract.

**Exit**

All information is to be stored on MOD devices and in MOD locations (no information to be stored on either, company laptops or personal device). The supplier should make adequate preparation for handover and knowledge transfer to new supplier. A key element to this contract will be information management and knowledge transfer. The supplier will ensure that all relevant documentation is created and stored within MOD configuration management policy.

3 months prior to the end of the contract the supplier will:

Update a statement of work that details the current activities.

Generate a service transition plan.

Conduct a documents, information, and knowledge transfer to the successful tenderer.

Correctly store and archive all information on MoD CIS in line with Navy Digital Information Management policy.

Work with Navy Digital to ensure preparations for a smooth transition in service.

**Software**

MoD ICT will be used throughout this service and supplier ICT is not to be used for the delivery of this service. The supplier must ensure all personnel have the relevant security clearances to access necessary MoD ICT.

**IPR or Other Rights**

All IPR remains with MoD.

**Acronyms**

Any acronyms or Capitalised Terms should be listed with a description of what they are.

Annex A

To SOR

30th August 2023

**Statement of Technical Need**

The following statement of technical need is designed to give the reader a full in depth understand of the activities required to deliver the technical service specified in the main body of this SOR.

**Output 1**

**ICT Build Services**

**Service Overview**

Working as part of the MCSU ICT team, this output requires the provision of and support ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelinesand within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Handle ‘NCSC’ crypto classified up to secret and configure VIASAT Eclypt core/freedom drives.

* Maintain the image library for the core set of MCSU catalogue systems and ensure that the library of images is regularly updated to keep them in compliance with the Security Operating instructions (SyOPs).

* Manage a library of software used on the array of systems delivered by MCSU and ensure that the version number is regularly updated.

* Build ICT systems classified up to secret, whether that be from the set MCSU catalogue of systems or specialist individual systems all in accordance with their SyOPs.

* Provide through life support, investigating any faults/issues that the end user’s experience, leading to sourcing, and implementing the solution.

* Provide assistance to end users regarding the correct usage of their systems to ensure it is being used in accordance with their SyOPs.

* Spec and technically evaluate computer hardware as to whether it is fit for purpose and if it can be used by MCSU/Royal Navy.

* Provide technical assistance to the MCSU service desk when required.

* To manage and continuously update the MCSU password database that is used to store all passwords for users to access via the MCSU service desk upon receiving of any system built by MCSU ICT.

* Quality of Service, peer review check by another member of ICT build team to ensure system has been built to correct state.

* Potential if the ICT dockyard office comes to fruition that the build team will then be required to be spread across the two offices and will be providing a new service for drop in fixes for end users

**Additional Tasking**

* Maintain continuity across the service; liaise with the remainder of ICT for the delivery and support of ICT products.

* If tasked, give awareness to end users on the basic use of MCSU ICT provided systems, how to update their antivirus so it is in accordance with their (SyOPs). This awareness does not include detailed software specific training as this is the responsibility of the requesting users
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

* Continuously improve your knowledge for emergent technologies, hardware, software, and operating systems.

SC required as a Minimum

**Output 1**

**ICT Build Management**

**Service Overview**

Working as part of the MCSU ICT team, this output requires the provision of management across ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelinesand within the Navy Command (NC) Agile framework.

**Primary Tasking**

* ICT Build management oversees the ICT build service. This includes operating as the initial POC for enquiries and other support related tasks within MCSU and wider Navy Digital stakeholders.
* Ensure the workflow that comes though the ICT compliance and engineering team is completed against priorities and deadlines.
* Systems are completed in compliance to the Security Operating instructions (SyOPs).
* Be responsible for the ‘NCSC’ crypto signed out from the crypto custodian whilst the crypto is in possession of the ICT build team.
* Attend the daily MCSU ICT Scrum meetings to provide updates and assist in Incident rectification and Change Requests of MCSU provided ICT systems.
* Liaise with the ICT Compliance and Engineering office to identify any potential issues and finalise build specifications for jobs to be completed by the ICT build team.
* Work with the logistics team at MCSU to ensure the stock allocated for the jobs meets the technical specification needed.
* Ensuring that all the administrative aspects of the ICT build team are maintained and development in line with continuous service improvement principles.
* Liaise with other MCSU support teams that are involved in systems build such as Data Application Support (DAS) and ISR. Ensure that software from or for these organisations is the latest available.
* To create and maintain the required documents, for example AV guides that are distributed out with each system for the end users.
* To create each systems CIS Security Registration Document upon the completion of its build.
* Provide and maintain a Quality-of-Service system ensuring ICT build systems are checked prior to issuing to users.
* Maintain a log of all outgoing completed calls.
* Create a monthly update disc with the latest versions of any antivirus updates that will be passed to the MCSU SIO to distribute out to the RN fleet.
* Using remedy, update all the calls that are worked on at any stage by the ICT build team.
* Manage and populate the database with all the information related to the ‘NCSC’ crypto used.

**Additional Tasking**

* To train new build team members, so that they can learn the processes used by MCSU and how to correctly build the various systems, so they are in accordance with the system (SyOPs).
* If tasked, give awareness to end users on the basic use of MCSU ICT provided systems, how to update their antivirus so it is in accordance with their (SyOPs). This awareness does not include detailed software specific training as this is the responsibility of the requesting users.
* Liaise with MCSU ICT compliance and procurement as required for the selection of new replacement ICT hardware.
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

Maintain current knowledge of emergent technologies

SC required as a Minimum

**Output 2**

**MCSU ICT Programme Management**

**Service Overview**

Working as part of the MCSU ICT team, this output requires the provision of management across ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelinesand within the Navy Command (NC) Agile framework.

**Primary Tasking**

* MCSU ICT Programme Management ensure delivery of MCSU ICT hardware and software including security and applications to end users to fulfil the customer requirement as agreed to time, cost and quality.
* Provide Security and Risk Management advice and assistance to NC for accurate and timely submissions to the Defence Assurance Risk Tool (DART). Provide or assist with the compilations of Security Operating instructions (SyOPs) and other system accreditation documents for the contracted ICT deliverables.
* Ensure security and risk management issues are highlighted to the Command, Senior Responsible Officers (SRO’s)’s or Capability managers as required. Liaise with PSYA and Security as a Service to maintain RN CIS security alignment.
* Implement all Government and/or MOD mandated security applications/procedures on MCSU ICT and other ICT assets (by prior agreement). Where there is no managed service wrap and NC holds IT security and information risk, record the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset databases.
* Provide Technical and Project management direction for ICT projects. Run or support the MCSU ICT Change Working Group/Incident Management Scrums.
* Ensure Through Life Management (TLM) is in place for projects and systems provided by MCSU ICT for example Maritime Managed IT Equipment (MARMITE) and the Mobile Device Management System. Carry this out in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLCM, which will remain the responsibility of NC.
* Provide support to MCSU and ICT management for briefing ICT deliverables to internal and external departments and organisations.
* Provide support to MCSU and ICT management for the provision of Operational Level Agreements and Service Level Agreements relating to ICT provided hardware or software TLM.
* Oversee the MCSU ICT build team to ensure systems are correctly configured and accredited before release from MCSU.
* Work with Internal MCSU Stakeholders to support Continuous Service Improvement, Quality of Service and better align procedures and processes across the unit.

**Additional Tasking**

* If tasked, provide mobile support to NC ICT throughout the UK or abroad with appropriate notice (at prior arrangement and agreement of all parties to the contract (and at no cost to the RN).
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions from Official to Above Secret including strap level systems. that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance, and notices.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative, agile ways of working can be exploited to support published NC outputs.
* Liaise with the logistics department and Defence Courier Service for the inwards and outwards shipping of all ICT hardware and software to and from the MCSU Portsdown site and customer locations.
* If tasked work with external stakeholders as directed by service personnel or crown servants in the provision of ICT. This may include other TLB’s such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAE.
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

DV required as a Minimum

**Output 3**

**ICT Logistics**

**Service Overview**

The logistics section of the service is required to manage the storage and distribution of IT equipment for MCSU (Mainly ICT dept.), it is also responsible for the disposal of end of life and broken IT equipment. The logistics team are responsible for the initial registering of all IT equipment into the Navy Command Asset Register (NCAR).

**Primary Tasking**

* Processing New Receipts which include secure storage and/or issue of newly purchased IT equipment and accessories, actioning as advised by Procurement Team, updating Remedy and NCAR.
* Processing returns from units to ensure secure storage of returned assets, quick turnaround of repairs, secure storage of assets deemed suitable for 2nd use, correct disposal of recyclable assets not required to be held in store, correct destruction of media no longer required, updating Remedy, NCAR, Disposals listing and Destruction listing.
* Assigning assets to Remedy calls requested by ICT Management which includes applying asset labels to specific equipment, delivering assets to ICT Build Team, preparing kits as required (e.g., MIPE), updating Remedy and NCAR.
* Maintaining a register of vouchers (S549, QRED, MISC RV etc) on SharePoint (Refer to Logs SOPs) and maintaining office files that support receipts, issues, despatches, disposals and destruction.
* Packing and Despatch of assets from the ICT Build Team including using correct packing and labelling for parcels, timely despatch to Outward Shippers, Portsmouth Naval Base and/or via Parcel Force.
* Monthly stock count of specific asset types as required by ICT Procurement.
* Weekly email to ICT Procurement to advise on all Remedy calls that have been resolved.
* Provide Logistics support to other MCSU departments including LC2, NSWAN, CENTRIX, MDA and ISR teams.
* Develop and maintain close liaison with Portsmouth Naval Base Logistics team and customer service department for despatch and tracking of packages.
* Maintain close liaison with MCSU North and MCSU Devonport staff for despatch and delivery of packages to various units.
* To be qualified to complete paperwork and package Dangerous Goods for onward transfer.
* Operate and maintain the Logistics Van (Supplier Supplied) and record all journeys.

SC required as a minimum

**Output 3**

**ICT Logistics Management**

**Service Overview**

The Logistics section manages the storage and distribution of IT equipment for MCSU (Mainly ICT dept.), it is also responsible for the disposal of end of life and broken IT equipment. The logistics team are responsible for the initial registering of all IT equipment into the Navy Command Asset Register (NCAR).

**Primary Tasking**

* Processing New Receipts which include secure storage and/or issue of newly purchased IT equipment and accessories, actioning as advised by Procurement Team, updating Remedy and NCAR.
* Processing returns from units to ensure secure storage of returned assets, quick turnaround of repairs, secure storage of assets deemed suitable for 2nd use, correct disposal of recyclable assets not required to be held in store, correct destruction of media no longer required, updating Remedy, NCAR, Disposals listing and Destruction listing.
* Assigning assets to Remedy calls requested by ICT Management which includes applying asset labels to specific equipment, delivering assets to ICT Build Team, preparing kits as required (e.g., MIPE), updating Remedy and NCAR.
* Maintaining a register of vouchers (S549, QRED, MISC RV etc) on SharePoint (Refer to Logs SOPs) and maintaining office files that support receipts, issues, despatches, disposals and destruction.
* Packing and Despatch of assets from the ICT Build Team including using correct packing and labelling for parcels, timely despatch to Outward Shippers, Portsmouth Naval Base and/or via Parcel Force.
* Monthly stock count of specific asset types as required by ICT Procurement.
* Weekly email to ICT Procurement to advise on all Remedy calls that have been resolved.
* Provide Logistics support to other MCSU departments including LC2, NSWAN, CENTRIX, MDA and ISR teams.
* Develop and maintain close liaison with Portsmouth Naval Base Logistics team and customer service department for despatch and tracking of packages.
* Maintain close liaison with MCSU North and MCSU Devonport staff for despatch and delivery of packages to various units.
* To be qualified to complete paperwork and package Dangerous Goods for onward transfer.
* Operate and maintain the Logistics Van (Supplier Supplied) and record all journeys.

**Management Tasking**

* Receipting.

* + New Items: Advising Procurement Team of receipts, and processing as per Remedy call.
  + Equipment Returns: Liaison with Customer, instructing returns process and arranging customer delivery date where applicable.
* Storage.
  + Locate assets under secure storage at all times.
  + Prepare and locate last man out chits.
* Equipment Issues.
  + Assigning assets to Remedy Calls.
  + Despatches to all customers via Parcel Force; Naval Base; Logs Delivery or Customer Collection.
* Disposals.
  + Liaison with DSA, E -Cycle and Bonds Worldwide.
  + Arrangement of collection dates.
* Logistics Supplier Supplied Van
  + Maintain register of use.
  + Through Contract Admin Support, report vehicle defects and ensure vehicle service is in date.
  + Ensure timely refuelling add ad-blue additive as and when required. (Send expense claims via Contract Admin Support).
* Photocopier. Maintaining a Daily Register to include Start and End of Day readings.
* Equipment Use. Ensuring serviceability and safe use of equipment including
  + MHE – Pallets, Pallet Truck, Trolleys and Sack Truck.
  + Work at Height – Airport ladders and Elephant’s Feet.
  + Packing – Tape Dispenser and Pallet Strapping Kit.
* Packaging stock levels. Maintaining stocks of Bubble Wrap, Tape and Boxes.
* Defects. Reporting all defects to BSM team.

SC required as a minimum

**Output 4**

**ICT Mobile Device Management & Compliance Engineering**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Under the direction of the MDM Management, maintain, and develop MCSU’s in service Mobile Device Management (MDM) system.
* Deliver ICT hardware and software including security and applications to end users to fulfil the customer requirement as agreed to time, cost and quality.
* Provide Security advice and assistance to NC for accurate and timely submissions to the Defence Assurance Risk Tool (DART). Provide or assist with the compilations of Security Operating instructions (SyOPs) and other system accreditation documents for the contracted ICT deliverables.
* Implement all Government and/or MOD mandated security applications/procedures on MCSU ICT and other ICT assets (by prior agreement). Where there is no managed service wrap and NC holds IT security and information risk, record the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset database.

**Additional Tasking**

* If tasked, provide mobile support to NC ICT throughout the UK, with appropriate notice (at prior arrangement and agreement of all parties to the contract (and at no cost to the RN).
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions from Official to Above Secret including strap level systems. that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance, and notices.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative, agile ways of working can be exploited to support published NC outputs.
* Project Manage and support Project Management (PM) and Through Life Capability Management (TLCM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLCM, this will remain the responsibility of the authority.
* Provide technical and security input and updates for contracted ICT projects and wider IT projects, at meetings as required.
* Provide support to MCSU ICT Scrum to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide support to MCSU ICT Scrum to aid incident rectification of ICT provided systems.
* Liaise with logistics department and Defence Courier Service for the inwards and outwards shipping of all ICT hardware and software to and from MCSU Portsdown site and customer locations.
* Liaise with the ICT build team to ensure systems are correctly configured and accredited before release from MCSU.
* Liaise with ICT Crown servants if equipment provided will leave MCSU ICT without accreditation in place. Support the production of Operational level agreements. Identify and highlight risks involved to produce suitable Risk Balance cases by the Senior Responsible Officer to manage locally.
* If tasked, provide basic assistance or awareness of ICT provided systems, setting to work of the systems but not of the Software loaded to these systems.
* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLB’s such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAE. PSYA
* Work with Internal MCSU Stakeholders to support Continuous Service Improvement, Quality of Service and better align procedures and processes across the unit.
* Provide continuity for the MDM Management service
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

SC required as a minimum

**Output 4**

**MCSU ICT MDM Management**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Project Manage, maintain, and develop MCSU’s in service Mobile Device Management (MDM) system in line with NC Priorities.
* Provide direction and oversight to the MDM Engineer for the continued development and support of the MDM service and other MCSU ICT tasking.
* Deliver MCSU ICT hardware and software including security and applications to end users to fulfil the customer requirement as agreed to time, cost and quality.
* Provide Security advice and assistance to NC for accurate and timely submissions to the Defence Assurance Risk Tool (DART). Provide or assist with the compilations of Security Operating instructions (SyOPs) and other system accreditation documents for the contracted ICT deliverables.
* Implement all Government and/or MOD mandated security applications/procedures on MCSU ICT and other ICT assets (by prior agreement). Where there is no managed service wrap and NC holds IT security and information risk, record the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset databases.

**Additional Tasking**

* If tasked, provide mobile support to NC ICT throughout the UK, with appropriate notice (at prior arrangement and agreement of all parties to the contract (and at no cost to the RN).
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions from Official to Above Secret including strap level systems. that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance, and notices.
* Project Manage and support Project Management (PM) and Through Life Capability Management (TLCM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLCM, this will remain the responsibility of the authority.
* Provide technical and security input and updates for contracted MCSU ICT projects and wider IT projects, at meetings as required.
* Provide support to MCSU ICT Scrum to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide support to MCSU ICT Scrum to aid incident rectification of MCUS ICT provided systems.
* Liaise with the logistics department and Defence Courier Service for the inwards and outwards shipping of all ICT hardware and software to and from the MCSU Portsdown site and customer locations.
* Liaise with the MCSU ICT build team to ensure systems are correctly configured and accredited before release from MCSU.
* Liaise with MCSU ICT Crown servants if equipment provided will leave MCSU ICT without accreditation in place. Support the production of Operational level agreements. Identify and highlight risks involved to produce suitable Risk Balance cases by the Senior Responsible Officer to manage locally.
* If tasked, provide basic assistance or awareness of MCSU ICT provided systems, setting to work of the systems but not of the Software loaded to these systems.
* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLB’s such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAE.
* Work with Internal MCSU Stakeholders to support Continuous Service Improvement, Quality of Service and better align procedures and processes across the unit.
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

SC required as a minimum

**Output 5**

**ICT Network and Systems Engineering**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Provide support to NC ICT within the Portsmouth – Fareham area and exceptionally provide mobile support within the UK with appropriate notice (at prior arrangement and agreement of all parties to the contract).
* Implement all Government and/or MOD mandated security applications/procedures on NC ICT and other ICT assets (by prior agreement) where there is no managed service wrap and NC holds IT security and information risk, recording the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset database.
* Provide Security advice and assistance to NC for accurate and timely submissions to Defence Assurance Risk Tool (DART) and for the compilations of Security Operating instructions (SyOPs) and Risk Management and Accreditation Document Set (RMADS) and other system accreditation documents for the contracted ICT deliverables. Deliver all relevant security documentation to the customer in accordance with the NC authorised business case and agreed schedule.
* Provide knowledge, support and expertise for Government and/or MOD mandated security applications that have been installed/activated on contracted ICT deliverables.
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance and notices.
* Provide Project Management (PM) and Through Life Management (TLM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLM, this will remain the responsibility of the authority
* Provide support to MCSU Change Working Group to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide technical support to Security Working Groups (SWG) to assess security status of networks and systems and ensure compliance with all relevant Government and MOD regulations, guidance and notices.
* Implement and support non-MoDNET facilities to manage, update and assess the impact of patches and updates to Operating systems (OS) and applications for NC supported networks and stand-alone systems.
* Design, install, commission and support technical refresh of legacy networks within NC ensuring compliance with all relevant Government and MOD regulations, guidance and notices, giving consideration to system availability, business continuity and disaster recovery.
* Provide administration of networks/clients/software/applications on ICT where NC is the primary risk owner and where no other support exists, ensuring knowledge and expertise remains current for extant operating systems and networks installed and supported on behalf of the NC ICT.
* Provide support to MCSU ICT Scrum to aid incident rectification of ICT supported systems.
* Liaise with Logistics Department for the inwards and outwards shipping of al ICT hardware and software to and from MCSU Portsdown site and customer locations.
* Work with internal MCSU Stakeholders to support Continuous Service Improvement and better align procedures and processes across the unit.

**Additional Tasking**

* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLBs such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAe.
* If tasked provide basic training of ICT provided systems, setting to work of the systems, but not software loaded onto systems.
* Assist in the maintenance of the NCAR database through regular reporting to the NCAR Manager of changes in asset status of systems within area of responsibility.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative ways of working can be exploited to support published NC outputs.

DV required as a minimum

**Output 5**

**ICT Network and Systems Engineering**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Provide Mobile Engineer support to MCSU ICT as directed.
* Implement all Government and/or MOD mandated security applications/procedures on NC ICT and other ICT assets (by prior agreement) where there is no managed service wrap and NC holds IT security and information risk, recording the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset database.
* Provide Security advice and assistance to NC for accurate and timely submissions to Defence Assurance Risk Tool (DART) and for the compilations of Security Operating instructions (SyOPs) and Risk Management and Accreditation Document Set (RMADS) and other system accreditation documents for the contracted ICT deliverables. Deliver all relevant security documentation to the customer in accordance with the NC authorised business case and agreed schedule.
* Provide knowledge, support and expertise for Government and/or MOD mandated security applications that have been installed/activated on contracted ICT deliverables.
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance and notices.
* Provide Project Management (PM) and Through Life Management (TLM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLM, this will remain the responsibility of the authority.
* Provide support to MCSU Change Working Group to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide technical support to Security Working Groups (SWG) to assess security status of networks and systems and ensure compliance with all relevant Government and MOD regulations, guidance and notices.
* Implement and support non-MoDNET facilities to manage, update and assess the impact of patches and updates to Operating systems (OS) and applications for NC supported networks and stand-alone systems.
* Design, install, commission and support technical refresh of legacy networks within NC ensuring compliance with all relevant Government and MOD regulations, guidance and notices, giving consideration to system availability, business continuity and disaster recovery.
* Provide administration of networks/clients/software/applications on ICT where NC is the primary risk owner and where no other support exists, ensuring knowledge and expertise remains current for extant operating systems and networks installed and supported on behalf of the NC ICT.
* Provide support to MCSU ICT Scrum to aid incident rectification of ICT supported systems.
* Liaise with Logistics Department for the inwards and outwards shipping of al ICT hardware and software to and from MCSU Portsdown site and customer locations.
* Work with internal MCSU Stakeholders to support Continuous Service Improvement and better align procedures and processes across the unit.

**Additional Tasking**

* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLBs such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAe.
* If tasked provide basic training of ICT provided systems, setting to work of the systems, but not software loaded onto systems.
* Assist in the maintenance of the NCAR database through regular reporting to the NCAR Manager of changes in asset status of systems within area of responsibility.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative ways of working can be exploited to support published NC outputs.

SC required as a minimum

**Output 5**

**ICT Network and Systems Engineer**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* Provide support to NC ICT within the Portsmouth – Fareham area and exceptionally provide mobile support within the UK with appropriate notice (at prior arrangement and agreement of all parties to the contract).
* Implement all Government and/or MOD mandated security applications/procedures on NC ICT and other ICT assets (by prior agreement) where there is no managed service wrap and NC holds IT security and information risk, recording the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset database.
* Provide Security advice and assistance to NC for accurate and timely submissions to Defence Assurance Risk Tool (DART) and for the compilations of Security Operating instructions (SyOPs) and Risk Management and Accreditation Document Set (RMADS) and other system accreditation documents for the contracted ICT deliverables. Deliver all relevant security documentation to the customer in accordance with the NC authorised business case and agreed schedule.
* Provide knowledge, support and expertise for Government and/or MOD mandated security applications that have been installed/activated on contracted ICT deliverables.
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance and notices.
* Provide Project Management (PM) and Through Life Management (TLM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLM, this will remain the responsibility of the authority.
* Provide support to MCSU Change Working Group to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide technical support to Security Working Groups (SWG) to assess security status of networks and systems and ensure compliance with all relevant Government and MOD regulations, guidance and notices.
* Implement and support non-MoDNET facilities to manage, update and assess the impact of patches and updates to Operating systems (OS) and applications for NC supported networks and stand-alone systems.
* Design, install, commission and support technical refresh of legacy networks within NC ensuring compliance with all relevant Government and MOD regulations, guidance and notices, giving consideration to system availability, business continuity and disaster recovery.
* Provide administration of networks/clients/software/applications on ICT where NC is the primary risk owner and where no other support exists, ensuring knowledge and expertise remains current for extant operating systems and networks installed and supported on behalf of the NC ICT.
* Provide support to MCSU ICT Scrum to aid incident rectification of ICT supported systems.
* Liaise with Logistics Department for the inwards and outwards shipping of al ICT hardware and software to and from MCSU Portsdown site and customer locations.
* Work with internal MCSU Stakeholders to support Continuous Service Improvement and better align procedures and processes across the unit.

**Additional Tasking**

* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLBs such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAe.
* If tasked provide basic training of ICT provided systems, setting to work of the systems, but not software loaded onto systems.
* Assist in the maintenance of the NCAR database through regular reporting to the NCAR Manager of changes in asset status of systems within area of responsibility.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative ways of working can be exploited to support published NC outputs.

**Output 6**

**ICT Security Support & Compliance Engineering**

**Service Overview**

Working as part of the MCSU ICT team, this output requires support to ICT capabilities for the Royal Navy. This is carried out in line with the MOD’s “Building Cyber Secure by Design Capabilities” guidelines and within the Navy Command (NC) Agile framework.

**Primary Tasking**

* As the MCSU ICT lead security advisor provide SME support to all elements of MCSU ICT and associated Projects.
* Provide Security advice and assistance to NC for accurate and timely submissions to the Defence Assurance Risk Tool (DART). Provide or assist with the compilations of Security Operating instructions (SyOPs) and other system accreditation documents for the contracted ICT deliverables.
* Deliver MCSU ICT hardware and software including security and applications to end users to fulfil the customer requirement as agreed to time, cost and quality.
* Implement all Government and/or MOD mandated security applications/procedures on MCSU ICT and other ICT assets (by prior agreement). Where there is no managed service wrap and NC holds IT security and information risk, record the relevant agreed details on the NC Asset Register (NCAR) or other authorised ICT asset databases.

**Additional Tasking**

* If tasked, provide mobile support to NC ICT throughout the UK, with appropriate notice (at prior arrangement and agreement of all parties to the contract (and at no cost to the RN).
* Provide technical evaluation and/or advice for ICT network/server/client/software designs; develop cost effective and innovative solutions from Official to Above Secret including strap level systems. that meet the user requirements as agreed in the relevant NC approved business case, compliant with all relevant Government and MOD regulations, guidance, and notices.
* Maintain current knowledge of emergent technology; conduct evaluations and provide suggestions for the continuous improvement and development of NC systems, in order that innovative, agile ways of working can be exploited to support published NC outputs.
* Project Manage and support Project Management (PM) and Through Life Capability Management (TLCM) for projects and NC Assets within the remit of the contract in accordance with the MOD Acquisition Operating Framework (AOF). Excluding financial aspects of TLCM, this will remain the responsibility of the authority.
* Provide technical and security input and updates for contracted MCSU ICT projects and wider IT projects, at meetings as required.
* Provide support to MCSU ICT Scrum to assess/evaluate Requests For Change (RFC) and where applicable provide support to the Operational and Business Change Teams to refine requirements and identify solutions.
* Provide support to MCSU ICT Scrum to aid incident rectification of MCUS ICT provided systems.
* Liaise with the logistics department and Defence Courier Service for the inwards and outwards shipping of all ICT hardware and software to and from the MCSU Portsdown site and customer locations.
* Liaise with the MCSU ICT build team to ensure systems are correctly configured and accredited before release from MCSU.
* Liaise with MCSU ICT Crown servants if equipment provided will leave MCSU ICT without accreditation in place. Support the production of Operational level agreements. Identify and highlight risks involved to produce suitable Risk Balance cases by the Senior Responsible Officer to manage locally.
* If tasked, provide basic assistance or awareness of MCSU ICT provided systems, setting to work of the systems but not of the Software loaded to these systems.
* If tasked work with external stakeholders as directed by service personnel or crown servants. This may include other TLB’s such as DES Ships or MOD collaborative agencies such as DSTL and can include industry partners for example BAE.
* Work with Internal MCSU Stakeholders to support Continuous Service Improvement, Quality of Service and better align procedures and processes across the unit.
* Provide continuity for the ICT Programme Managemant during absences for meetings and MCSU ICT scrums.
* Stay in date with RN mandatory training courses, that are applicable to civilian staff and contractors, which includes cultural awareness, health and safety, and equality and diversity courses.

DV required as a Minimum

**Output 7**

**Navy Command Asset Register Management**

**Service Overview**

The Navy Command Asset Register (NCAR) is a key element in the maintenance of the Information Assurance Maturity Model (IAMM) accreditation and a Data Authority for the determination of Security Risks across Royal Navy and third-party supplied assets deployed across all Navy Command units.

**Tasking:**

* Database Sponsor and Subject Matter Expert (SME) of the NCAR, identifying and reporting functionality issues, identifying and evaluating potential additional functionality requirements, and liaising with the Commercial supplier and Navy Digital Support Team (NDST) to ensure delivery, implementation and maintenance.
* Maintain an Administration user guide and assist with the troubleshooting of issues occurring with front-end or back-end services (back-end services, including data backups, network links, and server updates are provided by NDST).
* Database Administration, controlling and restricting data exports, creating and amending user accounts to enable the user to see the data that they “need to know”, adding data and amending data as required.
* Database Administration, be the focal point for the import of data from different Data Authorities, and liaise with NC Procurement, IT Security Officers, Defence Accreditation Reporting Tool (DART), Principal Security Advisors (PSyA), Third Party suppliers, Manufacturers, RN and TLB Desk Officers, Defence and Equipment Service (DE&S), and FGEN/Abbeywood) ensuring all data is accurate, comprehensive, and complete.
* To inform the Military Tasking Equipment (MTE) onload and offload process of assets held, to enable agility in the supply of operational equipment deficiencies, to identify excess operational assets held.  Assist with expedient asset procurement and onload, as required, as directed by FGEN/Abbeywood.
* Evaluate, design, develop, adapt and maintain the front-end service of the Navy Command Asset Register (NCAR).  The front-end service includes the website landing screen and associated web pages which form the main client interface.
* Evaluate, implement and develop additional Software Licencing tracking functionality to enable NC to precisely track purchased licences (number and location), to comply with licence agreements in place at the time of purchase, and to recover and re-use licences when an asset is removed from service.
* Act as the NC point of contact for all NCAR issues, providing leadership, advice, reports to named deadlines and specific parameters, in order to maintain IAMM (or similar) accreditation.
* Assist NC, by liaison with Project Kraken, Project Nelson, NDST and the Commercial software supplier, to provide status reports of asset holdings to include Information Assurance, levels of Accreditation, Software Licencing, Financial value and tracking, and the Government Greening Strategy (e.g., power use, disposals weights and composition).
* Export Asset data, on a monthly basis, about NC supplied, standalone (assets that cannot be auto discovered on a network) assets to the centrally based Defence Digital Operational Service Management (DD OSM) Configuration Management Database, with the assumption that DD OSM convert the donated data into their own format for upload.
* Ensure system administrators of connected networks comply with DD OSM network auto-discovery, and provide advice for how to engage with the process
* Ensure accurate maintenance of the NCAR System list, identifying new systems, requesting accreditation details, and ensuring all systems record information is captured. Ensure that accreditation detail is linked to individual assets.
* Conduct periodic audits of assets to identify asset obsolescence due to Security risk (in response to a Data Authority request), financial depreciation, or age, and mark those records with a Condition tag, highlighting to RN that those assets need to be withdrawn and replaced.
* Contribute to Configuration Management by extracting data from asset build records, logistics receipt and despatch records, and procurement records in order to improve the identity of risk.
* Support client requests for user accounts, import and export of data, maintaining a user guide and supplying additional telephone training for the NCAR and asset security as required.  Encouraging users to comply with Security policies, to conduct spot-checks of assets, to seek Security Accreditation and provide further historical information in the event of Security Investigations.

Sc required as a minimum