**INVITATION TO TENDER**

**(OPEN PROCEDURE)**

**FOR**

**Provision of IT Security Solutions (2025)**

NMRNO.2025.008

The National Museum of the Royal Navy

HMS Naval Base (PP66)

Portsmouth

PO1 3NH

**Version 2025.01 (PA23)**

Table of Contents

[Section 1 3](#_Toc204077531)

[Introduction 3](#_Toc204077532)

[Introduction to the NMRN 3](#_Toc204077533)

[The Authority’s Requirement 4](#_Toc204077534)

[Preliminary Market Engagement 4](#_Toc204077535)

[The Procurement Timetable 4](#_Toc204077536)

[Key Dependencies 5](#_Toc204077537)

[Contract Risks 5](#_Toc204077538)

[Contract Terms 5](#_Toc204077539)

[Section 3 6](#_Toc204077540)

[How to Respond to this Opportunity 6](#_Toc204077541)

[Section 4 7](#_Toc204077542)

[Requests for Clarification 7](#_Toc204077543)

[Section 5 8](#_Toc204077544)

[Tender Assessment and Evaluation 8](#_Toc204077545)

[Section 6 10](#_Toc204077546)

[Structure and Format of Response 10](#_Toc204077547)

[Section 7 11](#_Toc204077548)

[Terms and Conditions of Tender 11](#_Toc204077549)

[Annex A 15](#_Toc204077550)

[Specification / Scope of Requirement 15](#_Toc204077551)

[Annex B 20](#_Toc204077552)

[Tender Evaluation Criteria 20](#_Toc204077553)

[Annex C 22](#_Toc204077554)

[NMRN Standard Terms and Conditions 22](#_Toc204077555)

[Annex D 23](#_Toc204077556)

[TENDER SUBMISSION DOCUMENT 23](#_Toc204077557)

[Response to Quality Evaluation Criteria 27](#_Toc204077558)

[Annex E 33](#_Toc204077559)

[Glossary 33](#_Toc204077560)

[Annex F 34](#_Toc204077561)

[Form of Tender 34](#_Toc204077562)

[Annex G 36](#_Toc204077563)

[Certificate of Non-Collusion and Non-Canvassing 36](#_Toc204077564)

[Annex H 37](#_Toc204077565)

[Commercially Sensitive Information 37](#_Toc204077566)

Section 1

Introduction

* 1. This Procurement is being conducted in accordance with the Act using the Open Procedure. This document describes how the Procurement will be conducted, including details of the associated Procurement timetable, participation and award criteria and how to respond to this opportunity. Suppliers are strongly encouraged to read this document before preparing their submission.
  2. This document has been prepared to assist Suppliers in deciding whether to participate in this Procurement. **Please read this document carefully, as failure to comply with this document may result in exclusion from the Procurement and/or the rejection of any submission.**
  3. This document should be read in conjunction with the Tender Notice and any other Procurement documents which have been made available at this stage of the Procurement.
  4. The Authority reserves the right to issue updated versions of this document to Suppliers as and when the need arises, together with any changes to the Procurement or any other new information.
  5. **Please read and ensure compliance with the Procurement terms and conditions contained in Appendix A.**
  6. Common terms and expressions shall have the meanings ascribed to them in the glossary in Appendix E.
  7. All references to a ‘section’ are to a section in the Act unless otherwise stated.
  8. All references to a ‘paragraph’, ‘appendix’ or ‘annex’ are to a paragraph, appendix or annex of this document unless otherwise stated.
  9. All references to dates and times within this document shall be interpreted in accordance with the United Kingdom time zones applicable at the date of the Procurement (i.e. GMT/BST).
  10. **All suppliers bidding for this tender MUST sign up to the Central Digital Platform (CDP) to be eligible to bid for this tender. Guidance can be found here;** [**Central Digital Platform - factsheet (HTML) - GOV.UK**](https://www.gov.uk/government/publications/procurement-act-2023-short-guides/central-digital-platform-factsheet-html)
  11. **The link for registration can be found here;** [**Find a Tender**](https://www.find-tender.service.gov.uk/Search) **it will provide you with a unique organisation identifier reference.**
  12. **When sending your submission in, please share your supplier information share code with us, or send the PDF version of this from the Find a Tender website.**

Introduction to the NMRN

* The National Museum of the Royal Navy (“the National Museum”) was established in 2008 and is the holding company of the National Museum of the Royal Navy Group. The Group’s unique and historically significant Royal Naval collections, ships and aircraft are located and displayed in museums at;
  + *National Museum of the Royal Navy in Portsmouth (including HMS Victory, HMS Warrior and HMS M33 and the national collection for the Royal Marines)*
  + *Fleet Air Arm Museum in Yeovilton*
  + *Royal Navy Submarine Museum (including HMS Alliance) and Explosion! The Museum of Naval Firepower in Gosport*
  + *National Museum of the Royal Navy Hartlepool (including HMS Trincomalee)*
  + *HMS Caroline in Belfast*

|  |  |
| --- | --- |
| **Our Vision** | *To be the world’s most inspiring Naval Museum, linking Navy to Nation* |
| **Our Mission** | *Inspiring enjoyment and engagement with the story of the Royal Navy and its role in shaping both our nation and the modern world.* |
| *Learn more about the NMRN on our website;* [*https://www.nmrn.org.uk/*](https://www.nmrn.org.uk/) | |

The Authority’s Requirement

* 1. Annex A and any relevant Appendices details the specification or scope of requirement against which your Tender will be evaluated.

Preliminary Market Engagement

* 1. The NMRN have undertaken preliminary market engagement to help inform the scope of requirement through conversations with the NMRN’s IT Support provide ROCK IT. As well as individual discussions with a number of vendors.

The Procurement Timetable

* 1. The timetable for the Procurement is set out in the following table (the Procurement Timetable). Deadlines for the submission of responses to the Authority are shown in bold. Failure to meet these deadlines will result in a Supplier’s submission not being considered unless there are exceptional mitigating circumstances such as a technical failure in connection with the NMN Tenders Inbox

|  |  |  |
| --- | --- | --- |
| **IT Security Provision- Open Procedure** | | |
|  | | |
| 1 | **Issue of Invitation to Tender Document** | Tuesday 22nd July 2025 |
| 3 | **Final date for Clarification Questions/Requests for additional information** | Midday (1200)  Friday 8th August 2025 |
| 4 | **Submission Deadline** | Midday (1200)  Monday 18th August 2025 |
| Post Submission of Open Procedure- | | |
| 5 | **Evaluation Moderation of ITTs** | Week Commencing 18th August 2025 |
| 6 | **Post Submission Interviews including demos.** | Week Commencing 25th August 2025 or 1st September |
|  | ***The below dates are subject to change with timeline of post-submission interviews*** | |
| 7 | ***Award Summary Notices Issued and Standstill Begins*** | Week Commencing  25th August or 1st September 2025 |
| 8 | ***Earliest Commencement of Contract after Standstill Period Ends and*** | Week Commencing  1st September 2025 or 8th September 2025 |
| 9 | ***Contract Award Notice Issued*** | Week Commencing  1st September 2025 or 8th September 2025 |

|  |  |
| --- | --- |
| **Site Visits, Tenderer Interviews and Clarification Questions** | |
| **Post- Submission-Tenderer Interviews** | The NMRN may, at its discretion, decide to interview Tenderers to further the tendering process. It is envisaged that interviews, if required by the NMRN, will take place during the week commencing **Week Commencing 25th August 2025 or 1st September 2025.**  **The NMRN would like to interview a minimum of 3 suppliers and maximum of 5 per Lot.**  The NMRN reserves the right to amend this timetable. Tenderers should ensure that key members of their delivery team are able to attend the interviews. |
| **Post-Submission Clarifications.** | During the evaluation period, the NMRN reserves the right to seek further information from the Tenderers to assist in its consideration of the Tenders; this may take the form of post-submission clarification meetings or written clarifications. |

* 1. Please note that the Authority reserves the right, in its absolute discretion, to amend the Procurement Timetable or extend any time period in connection with the Procurement. Any changes to the Procurement Timetable will be notified simultaneously to the Suppliers.

Key Dependencies

* 1. This tender opportunity is contracted to NMRN Operations as the contracting authority, the NMRN operate multiple sites as set out in this tender documentation. It is a joint partner in Portsmouth Historic Dockyard Operations (PHD Operations) alongside the Mary Rose Trust which the IT Security Solution(s)

Contract Risks

* 1. This tender opportunity follows the previous IT Hardware Purchase tender (NMRNO.2025.004) which the first stage of this IT Infrastructure Upgrade Project. This opportunity can be seen here; [Purchase of IT Infrastructure Hardware - Find a Tender](https://www.find-tender.service.gov.uk/Notice/020225-2025)
  2. Any delay or non-award of this tender will have impact on the upgrade project itself, with requirement to either go back out to tender or seek alternative appointment through internal approval procedures in the NMRN. As the provisions stated in this tender are to be implemented alongside the hardware installation.

Contract Terms

* 1. Annex C and any relevant Appendices details the NMRN Standard Contract Terms and Conditions against which your Tender will be contracted.

Section 3

How to Respond to this Opportunity

3.1 Construction of Tenders

3.1.1 Your Tender is to be written in English, using either Calibri/Arial/Aptos in a minimum font size 11.

3.1.2 Prices must be in **£GBP** ex VAT. The NMRN prefers for this appointment to have fixed for the initial 3-years. A price breakdown must be in the Tender.

3.1.3 Please provide your pricing proposal including the fee, payment dates, and other relevant sections such as a detailed breakdown, resource allocation as appropriate to the tender. It should be clearly labelled within your tender submission.

3.1.4- To assist the NMRN’s evaluation, you must set out your Tender response in accordance with Section 4 (Tender Evaluation).

3.2 Submission of your Tender

Your completed response should be submitted by the due date and time required:

Date: Monday 18th August 2025

Time: 1200 Midday

Responses should be submitted in an electronic format addressed to: [tenders@nmrn.org.uk](mailto:tenders@nmrn.org.uk)

Please ensure your submission has been received by keeping a copy of the automatically generated read receipt from the mailbox. If a submission is undeliverable for any reason, you will need to supply evidence in order that submissions can be considered.

* **It is the sole responsibility of the Tenderer to deliver their response and submission pack as specified and to ensure that their response has been received. It is suggested that this may achieved by setting either a Delivery Receipt or a Read Receipt.**
* The NMRN takes no responsibility for identifying any clerical errors or misunderstanding in any tenders submitted. Tenderers must therefore ensure that the content of any Tender submitted is complete and accurate.
* Please be aware that on occasions the NMRN IT Security settings may potentially block emails or submissions, please ensure to communicate prior to the submission deadline through clarifications registering interest in the tender. This is checked post-deadline.
* If you have received **no response** from the NMRN regarding your tender submission by **1700 (5pm)** of the date of the tender returns (excluding weekends) please email [procurement@nmrn.org.uk](mailto:procurement@nmrn.org.uk) or [enquiries@nmrn.org.uk](mailto:enquiries@nmrn.org.uk) citing the name of the tender you have submitted for. Or alternatively call; *02392891370 Ext: 2042* to speak to the Procurement Officer. Please leave a voicemail if the call is unable to be answered.

3.2.1 Your Tender and any ITT Documentation must be submitted electronically via the ‘Central Digital Platform’ (CDP) portal by Midday (1200) Monday 18th August 2025. The NMRN reserves the right to reject any Tender received after the stated date and time. Hard copy, paper or delivered digital Tenders (e.g. email, DVD) are no longer required and will not be accepted by the NMRN. Tenderers are required to submit an electronic online Tender response to ITT NMRNO.2025.008.

3.2.2 The NMRN may, in its own absolute discretion allow the Tenderer to rectify any irregularities identified in the Tender by the NMRN or provide clarification after the Tender return date. For example, this may include, but is not limited to, redacting pricing information in the unpriced copy of the tender, rectifying, or providing clarification in relation to a corrupt or blank document. Tenderers will be provided with instructions via the ‘Central Digital Platform’ (CDP)portal on how they can correct such irregularities which must be completed by the deadline set. The NMRN will cross reference the amended Tender with the original Tender submitted to the ‘Central Digital Platform’ (CDP) portal before the Tender return date to ensure that no other amendments, other than in relation to the specific irregularity/clarification communicated by the NMRN, have been made. Should Tenderers make additional amendments to the Tender other than those relating to the specific irregularity/clarification communicated to the Tenderer by the NMRN, this will result in a non-compliant bid.

3.2.3 You must not upload any ITAR or Export Controlled information as part of your Tender or ITT documentation into the ‘Central Digital Platform’ (CDP) portal. You must contact *Procurement Officer on 02392891370 ext 2042* to discuss any exchange of ITAR or Export Controlled information. You must ensure that you have the relevant permissions to transfer information to the NMRN.

3.2.4 Your Tender must be compatible with MS Word and other MS Office applications.

### **3.3 Variant Bids**

3.3.1 Subject to the submission of a compliant tender, Tenderers may also submit an alternative price and method for provision of the services or goods which NMRN, at its sole discretion, may or may not pursue.

3.4 Confidentiality

3.4.1 NMRN will not disclose to any third-party information that is supplied in tenders that is marked as confidential. All other information supplied by Tenderers to NMRN will similarly be treated in confidence except that references may be sought from banks, existing or past clients, or other referees submitted by the Tenderers.

3.5 Conflict of Interest

3.5.1 Tenderers are required to confirm that they are not aware of any conflict of interest or any circumstances that could give rise to a conflict of interest in the performance of the proposed Contract.

3.6 Consortia

3.6.1 Bids from multi-disciplinary organisations and specially formed consortia are encouraged, but all organisations in specially formed consortia must be identified in the response to the ITT. Each group or consortium will be required to nominate a lead person with whom NMRN can contract or form themselves into a single legal entity before contract award. In the case of group Tenderers or consortia, each service provider will be required to become jointly and severally responsible for the contract before acceptance.

3.6.2 If the tenderer is a group Tenderer or consortium, each member of the consortium must be identified separately as part of the response to this ITT.

3.6.3 If the tenderer is a member of a group of companies, they should provide information only about themselves and not the Group as a whole (except where Group information is specifically requested by the question).

Section 4

Requests for Clarification

* 1. Any requests for clarification relating to the Procurement must be submitted via the NMN Tenders Inbox, no later than the deadline in the Procurement Timetable at paragraph [15] above to allow the Authority sufficient time to respond prior to the closing date for receipt of submissions. The Authority will endeavour to respond to requests for clarification submitted in accordance with these requirements as soon as possible.
  2. The Authority reserves the right not to answer any requests for clarification submitted after the deadline set out in the Procurement Timetable at paragraph [15] above or submitted via any means other than the NMN Tenders Inbox.
  3. If Suppliers identify a technical issue with the NMN Tenders Inbox, they should contact the Authority without delay via the following contact point at:

**Procurement Officer**

[Procurement@nmrn.org.uk](mailto:Procurement@nmrn.org.uk) or by phone 02392 891370 ext 2042.

* 1. Where the Authority considers any requests for clarification to be relevant to the proper functioning of the Procurement, it will transmit to all other Suppliers (without reference to the identity of the Supplier which submitted the clarification question) the clarification question raised and the Authority's response, with the exception of those deemed confidential as provided below.
  2. If a Supplier considers that its request for clarification should be treated as confidential and not disclosed to other Suppliers, it must communicate this and the reason why to the Authority at the time of the submission of that clarification request. The Authority will advise the Supplier in advance of providing the clarification response if it considers that all or any part of the request for clarification cannot be treated as confidential, and will provide an opportunity for the Supplier to withdraw such aspects of the request for clarification.
  3. In such circumstances, the Supplier may either submit an amended request for the clarification to be treated as confidential, which would be considered by the Authority in the same manner as the original request, or raise a new request to be treated as a non-confidential request for clarification.
  4. It is the responsibility of each Supplier to monitor all clarifications issued by the Authority. The Authority accepts no liability for any Supplier's failure to keep abreast of clarifications issued.

Section 5

Tender Assessment and Evaluation

5.1 Evaluation of Tenders (Compliance)

5.1.1 You will have your tender response evaluated as set out in Annex B and scored in accordance with below:

**Stage 1: Receipt and Opening** - Tenders will be downloaded from [tenders@nmrn.org.uk](mailto:tenders@nmrn.org.uk) email inbox after the Closing Date. The NMRN firewall will be checked to ensure that all submissions are received including any attachments.

↓

**Stage 2:** **Compliance Check**

Each Tender will be checked for compliance with the requirements of this ITT. Tenders which are not substantially complete or which are non-compliant with the ITT may be excluded from further participation in the evaluation process or, at the NMRN’s discretion, Tenderers may be asked to provide clarification. In the case of the latter, a failure by the Tenderer to provide a satisfactory response within the deadline specified in the request for clarification may result in disqualification from the evaluation process. The NMRN reserves the right to evaluate Tenders before declaring them non-compliant.

↓

**Stage 3:** **Evaluation of Tender Responses** - Price and quality evaluation will be carried out in accordance with the published evaluation criteria

↓

**Stage 4:** **Score Review** - Review of quality and price scores

↓

**Stage 5:** **Final Evaluation Report and Recommendation** - A final evaluation report will be completed, recommending award.

5.1.2 Please note that the NMRN may require clarification of the answers provided or ask for additional information.

5.1.3 The response should be submitted by an individual of the organisation, company or partnership who has the authority to answer on behalf of that organisation, company or partnership.

5.1.4 Should the response be found to be erroneous or in any other way incorrect, the NMRN reserves the right to disqualify the candidate from the tender.

5.2 Evaluation of Tenders (Award)

5.2.1 In accordance with the Procurement Act 2023 and the Procurement Regulations 2024 the NMRN seeks to award the contract on the basis of the Most Economically Advantageous Tender. Tenders will be evaluated at Stages 3 and 4 in accordance with the following criteria and weightings and will be assessed entirely on your response submitted:

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Weighting** | **Demonstrated by** |
| **Quality including Methodology and Approach** | [100]% | Each criterion will be marked using the scale 0-10 and the specified weighting applied. The formula to calculate the weighted score will be:  *(marks awarded) x weighting*  *marks available*  For example if the weighting is 20% and the maximum mark is 5, and the mark received is 3, the weighted score would be:  *( 3 / 5 ) x 20 = 12*  NB**:** For the purposes of this calculation, weighting is expressed as a number not a percentage. |
| **Commercial**  **Price per Quality Score Points** | Price Only | In this approach a PQP is calculated for each bid by:   * determining the bid price; * determining the quality score for each bid, expressed as a whole number rather than as a percentage (though the whole number may still be points out of 100); and * dividing the bid price by the quality score to give an output price per quality point.   Price  –––––––––––––––––––––––––––––––––––  Quality score   * *For example, if a bid was £15,000 and the tenderer scores 75/100 the Price Per Quality score would be 200.*   The lowest ranked Price per Quality Score will be the Most Advantageous Tender based upon this. |

5.2.2 Scoring Model – Tender responses will be subject to an initial review at the start of Stage 3 of the evaluation process. Any tender responses not meeting mandatory requirements or constraints (if any) will be rejected in full at this point and will not be assessed or scored further. Tender responses not so rejected will be scored by an evaluation panel appointed by the NMRN for all criteria other than Commercial using the scoring model given in the table below:

|  |  |
| --- | --- |
| Points | Interpretation |
| 10 | **Excellent** –Overall the response demonstrates that the Tenderer meets all areas of the requirement and provides all of the areas evidence requested in the level of detail requested. This, therefore, is a detailed excellent response that meets all aspects of the requirement leaving no ambiguity as to whether the Tenderer can meet the requirement.  The response therefore shows: • Very good understanding of the requirement • Considerable competence demonstrated through relevant experience • Considerable insight into the relevant issues The response is also likely to propose additional value in several respects above that expected |
| 7 | **Good** -Overall the response demonstrates that the Tenderer meets all areas of the requirement and provides all of the areas of evidence requested, but contains some trivial omissions in relation to the level of detail requested in terms of either the response or the evidence. This, therefore, is a good response that meets all aspects of the requirement with only a trivial level ambiguity due the Tenderers failure to provide all information at the level of detail requested.  The response therefore shows: • Good understanding of the requirements • Sufficient competence demonstrated through relevant experience • Some insight demonstrated into the relevant issues |
| 5 | **Adequate** - Overall the response demonstrates that the Tenderer meets all areas of the requirement, but not all of the areas of evidence requested have been provided. This, therefore, is an adequate response, but with some limited ambiguity as to whether the Tenderer can meet the requirement due to the Tenderer’s failure to provide all of the evidence requested.  The response therefore shows: • Basic understanding of the requirements • Sufficient competence demonstrated through relevant experience • Some areas of concern that require attention |
| 3 | **Poor** – The response does not demonstrate that the Tenderer meets the requirement in one or more areas. This, therefore, is a poor response with significant ambiguity as to whether the Tenderer can meet the requirement due to the failure by the Tenderer to show that it meets one or more areas of the requirement.  There are reservations because of one or all of the following: • There is at least one significant issue needing considerable attention • There is insufficient evidence to demonstrate competence or understanding • The response is light and unconvincing |
| 0 | **Unacceptable** - The response is non-compliant with the requirements of the ITT and/or no response has been provided.  The response is significantly below what would be expected because of one or all of the following: • The response indicates a significant lack of understanding • The response fails to meet the requirement |

Section 6

Structure and Format of Response

6.1 Introduction

6.1.1 Your response to this tender document should follow the defined structure as outlined in Annex D. Your response will be used to evaluate and score the different sections of each proposal received. All parts of this section are deemed Essential and require response. **Failure to provide this information may result in your submission being disqualified:**

1. **The Suppliers Central Digital Platform Reference Number**
   1. **Suppliers can sign up here;** [**Find a Tender**](https://www.find-tender.service.gov.uk/Search)
2. **Annex D – Tender Submission Document**
3. **Annex E - Form of Tender**
4. **Annex F - Certificate of Non-Collusion**

Please supply relevant documentation with your submission. You are asked to answer questions fully and where indicated in the format required. Please do not provide additional attachments or documents where not requested to do so. These will not be read and will not be taken into account in the evaluation of your Tender. **Any tender not conforming to this requirement is likely to be disqualified.**

6.1.2 The response should be presented in A4 format with an easily readable font style and size.

6.2 Approach to the Contract (Quality Control)

6.2.1 Tenderer’s should describe how they will approach the implementation and performance of this contract with particular regard to the requirements outlined in the Specification / Schedule of Requirements (Annex A and its Appendices). Tenderer’s should outline their proposals for on-going quality control during the project and how they will remedy any failures.

6.3 Project Resourcing

6.3.1 Tenderer’s should describe the resources that they will be deploying on this contract if they are successful, stating whether any staff resources are currently in place or will require to be recruited. They should also give indications as to the background and knowledge of key personnel who will be deployed in the delivery of this contract.

6.3.2 Explain any sub-contract arrangements that you will depend on to deliver the contract and explaining how you will manage this/these relationships with other stakeholders (if any). Any Lead Times between award of Contract and start of Services should be highlighted.

Section 7

Terms and Conditions of Tender

Procedural requirements

* 1. This document together with all other associated documents provided to Suppliers in connection with this Procurement contain procedural requirements which Suppliers must follow. Failure to comply with or follow any procedural requirement may result in the exclusion of the Supplier from the Procurement at the Authority’s sole discretion.

Central Digital Platform

* 1. **Suppliers that wish to participate in this Procurement are responsible for ensuring that the Central Digital Platform contains complete, accurate and up-to-date information about their organisation and any Associated Suppliers which are relevant for the purposes of this Procurement**. Suppliers must notify the Authority immediately if it is unable to register on the Central Digital Platform and/or provide accurate and up-to-date information via the Central Digital Platform.

Transparency

* 1. Suppliers should note that, in accordance with general transparency obligations and procurement law obligations under the Act, the Authority routinely publishes details of its procurement processes and awarded contracts. This includes, but is not limited to, the contract value, the identity of the successful Supplier, compliance with payment obligations and contract performance. Compliance with these obligations may involve the Authority taking steps without consultation with Suppliers. Where required under the Act, a copy of the contract will be published (subject to making any reasonable and proportionate redactions permitted under the Act).
  2. All central government departments and their executive agencies and non-departmental public bodies are subject to controls and reporting within government. In particular, they report to various government bodies including but not limited to the Cabinet Office and HM Treasury for all expenditure. The Authority reserves its absolute right to share within government any of the documentation/information submitted by Suppliers during this Procurement (including any information that a Supplier considers to be confidential and/or commercially sensitive).]
  3. Where required, the Authority will disclose on a confidential basis any information it receives from Suppliers during the Procurement to any third party engaged by the Authority for the specific purpose of assessing or assisting the Authority in assessing the Supplier’s submission. In providing such information the Supplier consents to such disclosure.

Modifying the Procurement

* 1. Neither the Tender Notice, this document nor any information given as part of the Procurement shall be regarded as a commitment or representation on the part of the Authority (or any other person) to enter into a contractual agreement.
  2. The Authority reserves the right to cancel the Procurement at any point and/or to choose not to award any contract as a result of this Procurement.
  3. Suppliers will remain responsible for all costs and expenses incurred by them, their staff, and their advisers or by any third party acting under their instructions in connection with this Procurement. For the avoidance of doubt, the Authority is not liable for any costs or expenditure resulting from any cancellation or amendment of this Procurement.
  4. The Authority reserves the right at any time:

a. to issue amendments, modifications or additional information to any documentation which forms part of this Procurement, including the Procurement terms and conditions contained in this Appendix A

b. to require a Supplier to clarify their proposal(s) and/or tender submission in writing and/or provide additional information – failure by a Supplier to respond adequately may result in their tender submission being rejected

c. to alter the Procurement Timetable for this Procurement.

d. to rewind and re-run any part of the Procurement on the same or alternative basis.

e. to amend the Procurement as described herein, including the number of stages and the number of Suppliers to be selected at any stage

Option to direct award

7.10 The NMRN reserves the right to Direct Award a procurement should the procurement process result in only one Applicant submit an acceptable tender.

Confidentiality and publicity

* 1. Save to the extent made publicly available by the Authority, the information in this document (together with all attachments and any other information communicated to Suppliers during the Procurement) is made available on the condition that it is treated as confidential information by the Supplier and is not disclosed, copied, reproduced, distributed or passed to any other person at any time except in order to comply with legal obligations or for the purpose of enabling a submission to be made to the Authority, provided that such person has given an undertaking prior to the receipt of the relevant information (and for the benefit of the Authority) to keep such information confidential.
  2. Suppliers must not take part in any publicity activities with any part of the media about this Procurement without obtaining the express prior written agreement of the Authority. When requesting prior written agreement, Suppliers are required to detail the proposed media coverage including format and content of any publicity.

Freedom of information and environmental information

* 1. The NMRN is not defined as a Public Authority under Schedule 1 of the Freedom of Information Act and we are not required to respond to your information requests
  2. You may find information of interest to you within the NMRN’s Annual Trustees’ Report and Statement of Accounts available on the NMRN’s or the Charity Commission’s websites.

Requirements on sub-contractors and consortium

* 1. If requested to do so by the Authority, a Supplier will be required to enter into a legal arrangement with other members of a consortium or with any parties which are relied on in order to satisfy the conditions of participation relating to this Procurement (in accordance with section 72 of the Act). Acceptance of this request shall be considered a mandatory requirement and failure to accept the same may result in the Supplier’s exclusion from the Procurement.

Parent company guarantee or other securities

* 1. The Authority reserves the right to require a parent company guarantee or alternative equivalent form of security should the Supplier be successful in this Procurement.
  2. Where the Supplier’s parent company is incorporated outside the United Kingdom, the Authority will require a legal opinion from an independent firm of lawyers practising in that jurisdiction (at the Supplier’s own cost and expense) as to the capacity/authority of the parent company to enter into the parent company guarantee and the enforceability of the terms of the parent company guarantee in the relevant overseas jurisdiction.
  3. Notwithstanding the above, the Authority may specify minimum contractual financial security requirements as appropriate having regard to the financial assessment undertaken during this Procurement. Where the Authority specifies any financial security requirements, acceptance of the requirements shall be considered a mandatory condition and failure to accept the same may result in the Supplier’s exclusion from the Procurement.

Non-collusion, non-canvassing

* 1. Any attempt by a Supplier or their advisers to influence the Procurement in any way may result in the exclusion of the Supplier, without prejudice to any other civil or legal remedies available to the Authority and without prejudice to any criminal liability that such conduct by a Supplier may attract.
  2. Specifically, Suppliers must not directly or indirectly at any time:

a. devise or amend the content of their submissions in accordance with any agreement or arrangement with any other person, other than in good faith with a person who is a proposed partner, subcontractor, consortium member insurance provider or provider of finance

b. enter into any agreement or arrangement with any other person as to the form or content of any other submission or offer to pay any sum of money or valuable consideration to any person to effect changes to the form or content of any other submission

c. enter into any agreement or arrangement with any other person that has the effect of prohibiting or excluding that person from submitting a response in this Procurement

d. canvass any employees, members or agents of the Authority in relation to this Procurement

e. attempt to obtain information from any of the employees, members or agents of the Authority or their advisors concerning another Supplier or submission

f. carry out any other co-operation or collusion with another Supplier or any other person which the Authority considers capable of undermining fair competition

* 1. Suppliers are required to complete and return Appendix G (Certificate of non-collusion and non-canvassing) noting that the Authority will be entitled to rely on the information provided in the certificate.

Conflicts of interest

* 1. Suppliers are responsible for ensuring that no actual, potential or perceived conflicts of interest (within the meaning of the Act) exist between themselves and the Authority or its advisers. Suppliers must notify the Authority immediately of any actual, potential or perceived conflict of interest.
  2. In the event of any actual, potential or perceived conflict of interest, the Authority shall in its absolute discretion decide on the appropriate course of action. The Authority reserves the right to:

a. exclude any Supplier that fails to notify the Authority of an actual, potential or perceived conflict of interest, or where an actual conflict of interest exists

b. request further information from any Supplier and require any Supplier to take reasonable steps to mitigate a conflict of interest. This may include requiring any Supplier to enter into a specific conflict of interest agreement with the Authority. Failure to do so may result in the Supplier being excluded from participating in, or progressing as part of, the Procurement process

* 1. The Authority strongly encourages Suppliers to contact the Authority as soon as possible using the NMN Tenders Inbox should it have any concerns regarding actual, potential or perceived conflicts of interest.

Conflict assessments

* 1. The Authority confirms that, prior to the issue of the Tender Notice in this Procurement, a conflict assessment has been prepared in accordance with the Act.

Intellectual property

* 1. Suppliers are reminded that all intellectual property rights, including copyright, in the documents and materials supplied by the Authority and/or its advisers in this Procurement, in whatever format, belong to the Authority, its advisers or the relevant owner/licensor. Suppliers shall not copy, reproduce, distribute or otherwise make available any part of these documents to any third party (except for the purpose of preparing a submission) without the prior written consent of the Authority. All documentation supplied by the Authority in relation to this Procurement must be returned or destroyed on demand, without any copies being retained by Suppliers.

Anti-competitive behaviour

* 1. Suppliers are reminded of their obligations under applicable competition laws. The Authority may require evidence from Suppliers that their arrangements are not anti-competitive and reserves the right to require any Supplier to comply with any reasonable measures which may be needed to verify that no anti-competitive arrangements are in place.
  2. Any evidence of anti-competitive behaviour may result in a Supplier being disqualified from the Procurement. The Authority also reserves the right to refer any suspected breaches of applicable competition laws to the relevant authorities including, but not limited to, the Competition and Markets Authority and the Serious Fraud Office.
  3. Suppliers should note that anti-competitive behaviour may result in the Supplier being excluded from bidding for contracts under Schedule 7, Paragraph 7 of the Act. Where a relevant decision has been made by the Competition and Markets Authority under the Competition Act 1998, the Supplier may also be excluded from bidding for contracts under Schedule 6, paragraph 41 and may be added to the debarment list and/or be liable for civil and/or criminal penalties.

Contract

* 1. A tender submission is an offer to enter into a contract on the terms of the contents of the submission. Notification of an award decision does not constitute acceptance by the Authority. Any document submitted by a Supplier shall only have contractual effect when it is contained within an executed written contract.
  2. The Supplier’s tender submission must remain valid for acceptance for a period of [90 days] from the date of its submission or until any procurement challenge/s have been resolved.

Supplier withdrawal

* 1. Suppliers may withdraw from the Procurement at any time before the tender submission deadline by providing written notification to the Authority via the NMN Tenders Inbox.

Modifying your Tender

* 1. Suppliers may modify their submitted prior to the submission deadline. The Authority will not open until after the submission deadline set out in the Procurement Timetable.

Supplier eligibility

* 1. Suppliers are reminded that the eligibility requirements in this document, Tender Notice and all other associated tender documents apply to the Procurement at all times.
  2. The Authority reserves the right to require any Supplier to provide such further information as the Authority may require (and for the avoidance of doubt, the Authority may make multiple requests) as to any issue addressed in the ITT, including, but not limited to, the economic and financial standing of the Supplier at any stage of the Procurement and prior to the notification of the award decision and/or the award of the contract.
  3. The Authority must be notified in writing via the NMN Tenders Inbox ([tenders@nmrn.org.uk](mailto:tenders@nmrn.org.uk)) promptly of any changes in the information that the Supplier has provided in its response to this Procurement (including but not limited to arrangements in relation to any Associated Suppliers) at any point before the entry into the Contract so that the Authority may assess whether the Supplier continues to satisfy the relevant conditions of participation and should continue to qualify for participation in the Procurement. For the avoidance of doubt, the Authority reserves the right to take such action as it deems appropriate in the light of its assessment of the updated information, including (but not limited to) excluding the Supplier concerned from the Procurement.

Supplier warranties

* 1. In responding to this invitation, the Supplier warrants, represents and undertakes to the Authority that:

a. it understands and has complied with the conditions set out in this document

b. all information, representations and other matters of fact communicated (whether in writing or otherwise) to the Authority by the Supplier, its staff or agents in connection with or arising out of the Procurement are true, complete and accurate in all respects, both as at the date communicated and as at the date of the submission of the response to this document

c. it has made its own investigations and undertaken its own research and due diligence, and has satisfied itself in respect of all matters (whether actual or contingent) relating to the invitation and has not submitted its response in reliance on any information, representation or assumption which may have been made by or on behalf of the Authority (with the exception of any information which is expressly warranted by the Authority)

d. it has full power and authority to respond to this document and to perform the obligations in relation to the contract and will, if requested, promptly produce evidence of such to the Authority

* 1. Suppliers should note that the potential consequences of providing incomplete, inaccurate or misleading information include that:

a. the Authority may exclude the Supplier from participating in this Procurement

b. the Supplier may be excluded from bidding for contracts under Schedule 7, Paragraph 13 of the Act

c. the Authority may rescind any resulting contract under the Misrepresentation Act 1967 and may sue the Supplier for damages

Tender Commercial Evaluation

* 1. Suppliers should note that bids where applicable which significantly exceed the advertised budget under ‘best technically affordable tender’ may be deemed non-compliant and lead to disqualification from the tender process. This is in accordance with Tender Evaluation Commercial Policy Statement.
  2. The NMRN may use Price per quality point (PQP) is an evaluation technique designed to make it easier to consistently and fairly compare bids of varying quality and price. It also makes it easier for evaluation panel to judge how they may score overall.

Annex A

Specification / Scope of Requirement

1. **Introduction**

The National Museum of the Royal Navy (NMRN), established in 2009, is the operator of attractions across six locations in the UK. The NMRN’s main headquarters are in Portsmouth, UK.

**It should be noted that the NMRN is a charitable trust and so should benefit from any available charitable discounts. Our charity number is 1126283.**

The NMRN has reviewed its current cyber security stack and is looking to implement further measures to protect its systems, data and people. Solutions to be implemented should complement current security measures and enhance our visibility, understanding and response to cyber threats within the IT environment. The National Museum is reviewing its supply arrangements to ensure that it is aware of what the market currently has to offer and is in a position to select a supplier that is best able to deliver the National Museum’s requirements over the next 3 – 5 years.

1. **Current Status**

The security measures currently in use by the NMRN include:

* Microsoft Defender for Business, included as part of Microsoft 365 Business Premium licensing
* Mobile Device Management and associated policy control through Microsoft Intune (Business Premium licensing)
* Fortigate 100F firewalls, soon to be replaced with SonicWall NSA4700 firewalls
* Microsoft 365 email security
* Microsoft 365 identity security
* URL content filtering
* Security Awareness Training

The NMRN operates 6 sites across the UK, with a centralised IT infrastructure at its Portsmouth headquarters. All sites are linked together using an MPLS network with the current Internet Service Provider. It is anticipated that we will move towards SD-WAN in the future to interconnect NMRN sites. The NMRN also has a single server in Microsoft Azure which communicates with the central infrastructure at the Portsmouth headquarters through a VPN tunnel.

Hybrid working is supported, so users of NMRN IT systems often work remotely. When working remotely, internal company data can be accessed via a VPN service (currently the Microsoft Azure VPN) on an NMRN managed device. Users may work on or off the VPN when working remotely, depending on what resources they need access to. Microsoft 365 services can also be accessed through NMRN managed devices or through BYOD, when certain conditions are met.

The NMRN currently supports around 400 Windows 11 and Windows Server (2022 and 2025) based devices. Across all internal networks, it is estimated that we have around 900 active IP addresses. Microsoft 365 services are widely used throughout the business. This includes Teams/SharePoint/OneDrive, Exchange, Azure/Entra, O365, Dynamics 365, Power Platform and Power BI. Entra Single Sign On is also configured on a number of 3rd party services. We currently have 228 licensed users on Microsoft 365, inclusive of mailboxes and OneDrive users. There are an additional 70 shared mailboxes.

Security solutions should be able to support the current and future IT infrastructure conditions and be scalable to accommodate any future increases in users, devices or IP addresses.

1. **Requirements, Contract Period and Budget**

This procurement has been split into multiple lots, representing the individual security requirements. Suppliers can bid on as many, or as few lots as they wish.

If suppliers are able to offer a holistic view of security threats and greater security benefits through solution packages on a unified platform and wish to bid on multiple lots as a result, please detail this in your response. Associated costs will need to remain within the budget limits set out in this ITT document.

The NMRN is looking for provision of the services for a minimum of three years and with potential for a maximum of five years (with a 3-year contract and an optional two-year extension subject to satisfactory performance).

The maximum budget available for this tender is **£238,000 over the initial 3-year period.** Individual lot prices are detailed within the individual lot requirements. Pricing proposals should be based on the numbers of devices, IPs, users and mailboxes in section 2, but pricing should also be broken down to per device/per user costs, where appropriate. The NMRN will confirm exact figures with the winning supplier(s) prior to contract commencement.

**Lot 1 – Managed Detect and Response**

The NMRN does not currently have an MDR service in place. It is anticipated that the service would commence during October 2025.

The NMRN is seeking a Managed Detect and Response (MDR) service to monitor activity across its IT estate and detect potential cyber threats. The MDR service should be paired with a suitable Extended Detection and Response (XDR) solution to provide maximum coverage across the IT environment, in particular Endpoint and Network Detection and Response. The solution should monitor, detect and respond to threats across the entire IT estate, including network, all servers and endpoints, tablets and smartphones. The MDR service should include, but not be limited to:

* 24/7/365 threat monitoring
* Active threat hunting
* Real-time threat detection and response
* Zero-day threat protection
* Incident response and investigation
* Alerting, reporting and regular communication
* Expert security analyst support

Implemented solutions should continuously monitor and detect both known and unknown (including zero-day) threats, anomalous activity, intercept and isolate malicious activity and prevent the lateral movement of threats across the NMRN’s IT environment. Automated actions should be possible, allowing the solution to autonomously respond to and contain threats.

The security solution should provide real-time threat detection, with alerting capabilities. The service should provide 24/7/365 monitoring by a Security Operations Centre (SOC) team and provide active threat hunting within the NMRN’s environment.

The service should include incident response capabilities, allowing the platform and SOC team to take swift actions to contain threats, isolate affected devices and prevent further spread of threats across the IT estate to mitigate risk. Forensic investigation should also take place following an incident so that the nature, origin and impact of cyber threats can be understood and prevented in the future.

Reporting capabilities should allow for ad-hoc and scheduled reports to be run from within the platform. The internal NMRN IT team would like to have visibility of the platform so that we can view threat dashboards and alerts in real-time.

Regular reporting from the service should provide detailed threat reports, including threat detections over the time period, steps taken for investigations, containment and remediation. Following an incident and forensic investigations, an incident report should be provided to the NMRN. Reporting should allow captured data to be queried, and threat trends identified. Logs and captured data within the solution should be retained for 90 days.

Finally, the NMRN would like to understand any additional benefits to the proposed MDR services. These may include, but are not limited to:

* Threat intelligence integrations allowing data to be fed from other sources, enhancing detection capabilities and identifying emerging threats.
* Integrations with the existing security stack, for example by ingesting firewall or Microsoft Defender logs to enhance the overall visibility of the security solution and better map attack paths.
* Continual learning allowing the solution to improve detection accuracy over time.
* The platform’s ability to identify and analyse suspicious activity in encrypted traffic.
* Whether the platform can do web content filtering based on rules, categories and specific URLs.

Suppliers should include a breakdown of costs for the MDR service, including:

* Set up and implementation costs
* Ongoing support costs
* Security solution cost breakdown (endpoint, network, SOC costs etc.)
* One-off engineer/analyst costs
* Ad-hoc additional support available in a threat situation
* Storage costs for log files (if applicable)
* Any other costs that contribute to the full cost.

The maximum available budget for **Lot 1 is £180,000** over the initial 3-year contract period.

**Lot 2 – Email Security Solution**

The NMRN currently has an email security solution in place, with the contract due to end on the 31st of October 2025. The new service should be in place to take over from this.

The NMRN uses Microsoft 365 Exchange for email services and the solution will need to be able to support this. The email security solution should also integrate with other security solutions, such as EDR, NDR and identity security solutions to enhance visibility of threats and help inform detection and response.

The solution should monitor inbound and outbound email traffic. The monitoring of lateral internal email traffic would also be beneficial. Features of the email security solution should include:

Inbound Email:

* Content and payload analysis – Content of an email, including the language and tone used, should be analysed to identify unusual or unexpected emails. URL links and attachments included in emails should also be analysed by the solution to identify suspicious, malicious or potentially dangerous content. Through its analysis, the solution should also be capable of detecting unknown and zero-day email threats.
* Sender verification – The solution should be capable of analysing and verifying the identity of a sender to help identify spoofing attempts. This should include SPF, DKIM and DMARC checks.
* Sender association – In addition to the above, the solution should analyse historical behaviour and previous association of a sender to understand the normal relationship between the parties involved in an email chain. This should help to uncover unusual email flows and supply chain attacks.
* Spam indicators – The solution should be able to identify spam email attempts, particularly when they are being distributed in bulk to multiple internal recipients.
* VIP users – the ability to identify and flag potential high priority email targets within the organisation, such as the CEO, and raise their profile within the security platform to adjust response actions accordingly.
* Previews – the ability to preview an email, including content and attachments, within a safe environment on the security platform
* Response actions – The solution should have the ability to autonomously respond to potential email threats depending on their severity of risk. Actions should include, but not be limited to, locking or removing links, converting or removing attachments, moving emails to junk, or holding emails to prevent delivery.
* Remediation actions – The ability to remediate an actioned email should be available so that emails actioned as false positives can be delivered to recipients without actions applied.
* Retrospective actions – The platform should have the ability to retrospectively apply actions based on new evidence. This should include the ability to ‘pull back’ emails from mailboxes post-delivery.

Outbound Email:

* Sensitive attachments and data loss – The solution should analyse outbound email traffic to identify potential data loss incidents and sensitive attachments being sent to unexpected recipients through association and historical behaviour analysis.
* Identifying possible email to personal addresses – Related to data loss, the solution should help to identify emails potentially being sent to personal email accounts.
* Email misdirection – The solution should be able to recognise potential email mis-directs being sent externally.
* Compromised accounts – The solution should be able to identify indicators of account compromise such as unexpected mass email sending to internal and external recipients and respond to these types of threats to prevent further damage.

Lateral Email:

* Internal to internal mail flow should be analysed to help identify unusual behaviour and mail flow that may indicate account compromise.

The email security solution should be capable of generating alerts for admins and reporting on the number of emails processed, applied response actions, threat indicators, plus potential data loss incidents. The ability to schedule automated summary reports should also be included.

The platform should retain logs for up to 90 days and allow the detailed inspection of emails processed by the platform. Log summaries should give a clear indication to admins of the analysis undertaken by the solution and any actions applied.

The maximum available budget for **Lot 2 is £38,000** over the initial 3-year contract period.

**Lot 3 – Microsoft 365 Identity Security Solution**

The NMRN currently has a Microsoft 365 identity security solution in place, with the contract due to end on the 31st of October 2025. The new service should be in place to take over from this.

The NMRN uses Microsoft 365 services throughout the business. This includes, Exchange, Azure/Entra, Microsoft Teams, SharePoint and OneDrive, Dynamics 365, Power Platform and Power BI. Entra Single Sign On is also configured on a number of 3rd party services. The identity security solution to be implemented should support these services to help monitor and protect accounts against malicious activity and compromise.

The Microsoft 365 identity security solution should enable real-time threat detection and response across our accounts and Microsoft 365 applications and services. Accounts and activity should be monitored to identify any unusual behaviour patterns and appropriate actions taken to mitigate potential threats. Account and activity monitoring should include, but not be limited to:

* Logon activity, such as time, location and frequency
* The use of unknown or new devices
* SaaS credential use
* Changes to recovery information
* Changes to multi-factor authentication (MFA) information
* Exchange activity such as creating mailbox rules
* SharePoint/OneDrive activity such as the creation of sharing links, permission grants, plus the accessing of, creation, modification and excessive download of files, providing data loss protection.

The solution should have the ability to respond to threats and perform actions including, but not limited to:

* Logging the user out
* Disabling the account
* Blocking suspicious IPs

The identity security solution should be capable of generating potential threat alerts and notifying admins of when actions have been applied. Reporting should also be possible on the activity processed, applied response actions, threat indicators, plus potential data loss incidents. The ability to schedule automated summary reports should also be included.

The platform should retain logs for up to 90 days and allow the detailed inspection of account activity processed by the platform. Logs should give a clear indication to admins of the analysis undertaken by the solution and any actions applied.

The maximum available budget for **Lot 3 is £20,000** over the initial 3-year contract period.

**Tender Information**

* Potential bidders are welcome to bid on either individual lots or multiple lots.
* The NMRN reserves the right to either award the lots individually or multiple to a single supplier if advantageous.

Annex B

Tender Evaluation Criteria

B.1 The Tender Evaluation criteria for this ITT is defined as follows:

Lot 1- Managed Detect and Response (MDR)

|  |  |  |
| --- | --- | --- |
| **Criteria** | | **Area Weighting** |
| **QUALITY Overall Weighting: 100%** | | |
| **1** | **Criteria 1-**   1. Please provide a case study for the proposed MDR service from an existing deployment where it has successfully detected, contained and prevented a high-risk cyber threat, such as Ransomware. Please detail:    1. How it was detected and investigation steps to confirm the threat.    2. Any actions taken for containment and prevention.    3. How the detection and response actions were communicated to the client.    4. Remediation steps taken/advised and support given to the client post-incident response. | 20% |
| **2** | **Criteria 2-**   * Please confirm your average threat detection and response times | 5% |
| **3** | **Criteria 3-**   1. Please detail your OLA and SLA for the proposed service. This should include:    1. The structure of the SOC team    2. Escalation paths for threat alerts, investigation and response    3. Escalation paths for the MDR service (account management) | 10% |
| **4** | **Criteria 4**   * Describe how the proposed MDR service supports the current requirements set out in Annex A, section 2. How will future requirements be supported? | 15% |
| **5** | **Criteria 5**   * Describe how the proposed MDR service meets the criteria set out in Annex A, section 4. How will you work with the NMRN to ensure requirements are met? | 20% |
| **6** | **Criteria 6**   * Please respond to the Appendix 1- Security Tender Questionnaire Lot 1 Tab-MDR Questionnaire | 30% |
| **PRICE** | | |
| 7 | **Price**   * Please provide a clear breakdown of the costs associated with your submission, this should include all known costs. These should be displayed as ex-VAT with a clear total cost displayed for the price assessment. | |
| **TOTAL** | | **100%** |

***Please note tenders are assessed on evaluation responses alone, prior knowledge or prior working relationships are not taken into consideration for the purposes of fairness.***

Lot 2- Email Security Solution

|  |  |  |
| --- | --- | --- |
| **Criteria** | | **Area Weighting** |
| **QUALITY Overall Weighting: 100%** | | |
| **1** | **Criteria 1**   * Please confirm the solutions average threat detection and response times | 15% |
| **2** | **Criteria 2**   * Describe how the proposed email security solution supports the current requirements set out in Annex A, section 2. How will future requirements be supported? | 20% |
| **3** | **Criteria 3**   * Describe how the proposed email security solution meets the criteria set out in Annex A, section 5. How will you work with the NMRN to ensure requirements are met? | 25% |
| **4** | **Criteria 4**   * Please detail the reporting capabilities of the system.   + Can automated reports be scheduled to provide summaries of the threats detected and actioned by the system? | 10% |
| **5** | **Criteria 5**   * Please respond to the Appendix 1- Security Tender Questionnaire- Lot 2 Tab – Email questionnaire | 30% |
| **PRICE** | | |
| **6** | **Price**   * Please provide a clear breakdown of the costs associated with your submission, this should include all known costs. These should be displayed as ex-VAT with a clear total cost displayed for the price assessment. | |
| **TOTAL** | | **100%** |

Lot 3- Microsoft 365 Identity Security Solution

|  |  |  |
| --- | --- | --- |
| **Criteria** | | **Area Weighting** |
| **QUALITY Overall Weighting: 100%** | | |
| **1** | **Criteria 1-**   * Please confirm the solutions average threat detection and response times | 15% |
| **2** | **Criteria 2**   * Describe how the proposed identity security solution supports the current requirements set out in Annex A, section 2. How will future requirements be supported? | 20% |
| **3** | **Criteria 3**   * Describe how the proposed identity security solution meets the criteria set out in Annex A, section 6. How will you work with the NMRN to ensure requirements are met? | 25% |
| **4** | **Criteria 4**   * Please detail the reporting capabilities of the system.   + Can automated reports be scheduled to provide summaries of the threats detected and actioned by the system? | 10% |
| **5** | **Criteria 5**  Please respond to the Appendix 1- Security Tender Questionnaire- Lot 3 Tab – Identity questionnaire section 4. | 30% |
| **PRICE** | | |
| **7** | Price   * Please provide a clear breakdown of the costs associated with your submission, this should include all known costs. These should be displayed as ex-VAT with a clear total cost displayed for the price assessment. | |
| **TOTAL** | | **100%** |

***Please note tenders are assessed on evaluation responses alone, prior knowledge or prior working relationships are not taken into consideration for the purposes of fairness.***

Annex C

NMRN Standard Terms and Conditions

* See in tender documentation pack the NMRN’s Standard Terms and Conditions
* Please be aware these are our full terms and conditions as a sample and does represent the final version for this tender. The NMRN will consider reasonable requests for negotiation post-award, these can be submitted as clarifications.
* The NMRN may also consider a contract from the winning bidder, if you wish to provide a sample contract relevant to this tender please submit this in your tender submission pack.

Annex D

TENDER SUBMISSION DOCUMENT

|  |  |  |
| --- | --- | --- |
| **Preliminary Questions** | | |
| **Question no.** | **Question** | **Response** |
| **1** | What is your name? (Supplier name) |  |
| **2a** | You must be registered on the central digital platform (CDP).  What is your central digital platform unique identifier?  Registration can be done here; [Find a Tender](https://www.find-tender.service.gov.uk/Search) |  |
| **2b** | **Please confirm and send your organisations Supplier Information Details attached to your submission pack as a PDF from Find a Tender Service.** |  |
| **3** | Please confirm if you are bidding as a single supplier (with or without sub-contractors) or as part of a group or consortium.  If you are bidding as part of a group or consortium (including where you intend to establish a legal entity to deliver the contract), please provide:  a. the name of the group/consortium  b. the proposed structure of the group/consortium, including the legal structure where applicable  c. the name of the lead member in the group/consortium  d. your role in the group/consortium (e.g. lead member, consortium member, sub-contractor) |  |
| **4** | Please confirm which lot(s) you wish to bid for? |  |
| **5** | Are you on the debarment list? |  |

* The Procurement Review Unit (formerly Public Procurement Review Service) allows government suppliers and potential government suppliers to raise concerns anonymously about unfair public sector procurement practice. Link here; [Public Procurement Review Service: scope and remit - GOV.UK](https://www.gov.uk/government/publications/public-procurement-review-service-scope-and-remit)

|  |  |  |  |
| --- | --- | --- | --- |
| **TECHNICAL ABILITY** | | | |
| **14** | Relevant experience and contract examples  Please provide details of up to three contracts to meet conditions of participation relating to technical ability set out in the relevant notice or procurement documents, in any combination from either the public or private sectors (which may include samples of grant-funded work).  Where this procurement is for goods or services, the examples must be from the past three years.  The named contact provided should be able to provide written evidence to confirm the accuracy of the information provided.  For consortium bids, or where you have indicated that you are relying on an associated person to meet the technical ability, you should provide relevant examples of where the associated person has delivered similar requirements. If this is not possible (e.g. the consortium is newly formed or a special purpose vehicle is to be created for this contract) then three separate examples should be provided between the principal member(s) of the proposed consortium or members of the special purpose vehicle or sub-contractors (three examples are not required from each member).  If you cannot provide at least one example of previous contracts, please provide an explanation for this and how you meet the conditions of participation relating to technical ability. | | |
| **Contract 1** | | | |
| Name of customer organisation who signed the contract | |  | |
| Name of supplier who signed the contract | |  | |
| Description of contract | |  | |
| Point of contact in the customer’s organisation | |  | |
| Position in the customer’s organisation | |  | |
| E-mail address | |  | |
| Contract start date | |  | |
| Contract completion date | |  | |
| Estimated contract value | |  | |
| **Contract 2** | | | |
| Name of customer organisation who signed the contract | |  | |
| Name of supplier who signed the contract | |  | |
| Description of contract | |  | |
| Point of contact in the customer’s organisation | |  | |
| Position in the customer’s organisation | |  | |
| E-mail address | |  | |
| Contract start date | |  | |
| Contract completion date | |  | |
| Estimated contract value | |  | |
| **Contract 3** | | | |
| Name of customer organisation who signed the contract | |  | |
| Name of supplier who signed the contract | |  | |
| Description of contract | |  | |
| Point of contact in the customer’s organisation | |  | |
| Position in the customer’s organisation | |  | |
| E-mail address | |  | |
| Contract start date | |  | |
| Contract completion date | |  | |
| Estimated contract value | |  | |
| **15** | **Experience of sub-contractor management**  Where you intend to sub-contract a proportion of the contract, please demonstrate how you have previously maintained healthy supply chains with your sub-contractor(s) (which may be the intended sub-contractor(s) for this procurement, or any others used previously).  The description should include the procedures you use to ensure performance of the contract. | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 7** | **Additional Questions including Project Specific Questions** | | |
| **Question no.** | **Question** | | **Response** |
| **7.1** | **Insurance**  Please self-certify whether you already have, or can commit to obtain, prior to the commencement of the contract, the levels of insurance cover indicated below: | |  |
| **Employer’s (Compulsory) Liability Insurance** = £5,000,000  *Policy Expiry Date:*  *Policy Reference:* | | Yes  No |
| **Public Liability Insurance** = £1,000,000  *Policy Expiry Date:*  *Policy Reference:* | | Yes  No |
| **Professional Indemnity Insurance** = £1,000,000  *Policy Expiry Date:*  *Policy Reference:* | | Yes  No |
| **Product Liability Insurance** = £1,000,000  *Policy Expiry Date:*  *Policy Reference:* | | Yes  No |
| Please note the insurance cover values shall not be less than the amounts detailed above for each and every claim.  \* It is a legal requirement that all companies hold Employer’s (Compulsory) Liability Insurance of £5 million as a minimum. Please note this requirement is not applicable to Sole Traders.  See the Health and Safety Executive website for more information:  <http://www.hse.gov.uk/pubns/hse39.pdf> | |  |
|  | **Use of Artificial Intelligence in Procurement Process & Proposal** | | |
| **A** | AI tools can be used to improve the efficiency of your bid writing process; however, they may also introduce an increased risk of misleading statements via ‘hallucination’.  Have you used AI or machine learning tools, including large language models, to assist in any part of your tender submission?  *This may include using these tools to support the drafting of responses to Award questions.* | Yes  No | |
| **B** | **If yes, please provide details: ………………** | | |
|  |  | | |
| **C** | Where AI tools have been used to support the generation of Tender responses, please confirm that they have been checked and verified for accuracy | Yes  No | |
| **d** | Are AI or machine learning technologies used as part of the products/services you intend to provide to the NMRN. | Yes  No | |
| **c** | If yes, please provide details: ……………… | | |
|  |  | | |

Response to Quality Evaluation Criteria

Technical/Quality Evaluation Criteria

* Each Criterion Question Response is clearly indicated to ensure it is clear for evaluation by the NMRN panel.
* Welcome to change fonts, but please keep these to a minimum of size 10 for response text.
* That no other part of the ITT is changed other than the Evaluation Criteria, as you’re welcome to separate this section only from the document.
* However, it must be clearly labelled for example- **“Supplier Name Response to Quality Evaluation Criteria”.**
* **That the word limit is just that, it is not a target.**
* It can be submitted as a PDF document or Word Document.

|  |  |  |
| --- | --- | --- |
| **Please indicate which Lot(s) you are bidding on** | | |
| **Lot 1** | **Lot 2** | **Lot 3** |
|  |  |  |

Lot 1- Managed Detect and Response (MDR)

|  |  |
| --- | --- |
| **Criterion 1** | 1. **Please provide a case study for the proposed MDR service from an existing deployment where it has successfully detected, contained and prevented a high-risk cyber threat, such as Ransomware. Please detail:**    1. **How it was detected and investigation steps to confirm the threat.**    2. **Any actions taken for containment and prevention.**    3. **How the detection and response actions were communicated to the client.**   **Remediation steps taken/advised and support given to the client post-incident response.** |
| Response  [1500-word limit] |  |
| **Criterion 2** | **Please confirm your average threat detection and response times** |
| Response  [1000-word limit] |  |
| **Criterion 3** | **Please detail your OLA and SLA for the proposed service. This should include:**   1. **The structure of the SOC team** 2. **Escalation paths for threat alerts, investigation and response** 3. **Escalation paths for the MDR service (account management)** |
| Response  [1500-word limit] |  |
| **Criterion 4** | **Describe how the proposed MDR service supports the current requirements set out in Annex A, section 2. How will future requirements be supported?** |
| Response  [1500-word limit] |  |
| **Criterion 5** | **Describe how the proposed MDR service meets the criteria set out in Annex A, section 4. How will you work with the NMRN to ensure requirements are met?** |
| Response  [1500-word limit] |  |
| **Criterion 6** | **Please confirm below that you have responded to the Appendix 1- Security Tender Questionnaire- Lot 1 Tab-MDR Questionnaire and provided this in your tender pack.** |
| Response  [250-Word] |  |

Lot 2- Email Security Solution

|  |  |
| --- | --- |
| **Criterion 1** | **Please confirm the solutions average threat detection and response times** |
| Response  [1500-word limit] |  |
| **Criterion 2** | **Describe how the proposed email security solution supports the current requirements set out in Annex A, section 2. How will future requirements be supported?** |
| Response  [1500-word limit] |  |
| **Criterion 3** | **Describe how the proposed email security solution meets the criteria set out in Annex A, section 5. How will you work with the NMRN to ensure requirements are met?** |
| Response  [1500-word limit] |  |
| **Criterion 4** | * **Please detail the reporting capabilities of the system.**   + **Can automated reports be scheduled to provide summaries of the threats detected and actioned by the system?** |
| Response  [1500-word limit] |  |
| **Criterion 5** | **Please confirm below that you have responded to the Appendix 1- Security Tender Questionnaire- Lot 2 Tab– Email questionnaire and provided this in your tender pack.** |
| Response  [250-Word] |  |

Lot 3- Microsoft 365 Identity Security Solution

|  |  |
| --- | --- |
| **Criterion 1** | **Please confirm the solutions average threat detection and response times** |
| Response  [1500-word limit] |  |
| **Criterion 2** | **Describe how the proposed identity security solution supports the current requirements set out in Annex A, section 2. How will future requirements be supported?** |
| Response  [1500-word limit] |  |
| **Criterion 3** | **Describe how the proposed identity security solution meets the criteria set out in Annex A, section 6. How will you work with the NMRN to ensure requirements are met?** |
| Response  [1500-word limit] |  |
| **Criterion 4** | * **Please detail the reporting capabilities of the system.**   + **Can automated reports be scheduled to provide summaries of the threats detected and actioned by the system?** |
| Response  [1500-word limit] |  |
| **Criterion 5** | **Please confirm below that you have responded to the Appendix 1- Security Tender Questionnaire- Lot 3 Tab – Identity questionnaire section 4. Questionnaire and provided this in your tender pack.** |
| Response  [250-Word] |  |

Annex E

Glossary

| **Defined term** | **Definition** |
| --- | --- |
| **Act** | means the Procurement Act 2023. |
| **Associated Suppliers** | means a Supplier who is associated with another Supplier if either (a) the Suppliers are submitting a tender together, or (b) the Authority is satisfied that the Suppliers will enter legally binding arrangements to the effect that the Supplier will sub-contract the performance of all or part of the Contract to the other, or the other Supplier will guarantee the performance of all or part of the Contract by the Supplier (as set out in section 22(9) of the Act). |
| **Authority** | means National Museum of the Royal Navy; as NMRN Operations |
| **Central Digital Platform** | means the online system defined by regulation 5(2) of the Procurement Regulations 2024 (SI 2024 No. 692). |
| **Contract** | means the contract to be entered into by the Authority with the successful Supplier. |
| **Key Performance Indicators or KPIs** | means the key performance indicators (KPIs) set out in this tender. |
| **Portal** | means the NMRN Tenders ([tenders@nmrn.org.uk](mailto:tenders@nmrn.org.uk)) used by the Authority for the purposes of this Procurement. |
| **Procurement Timetable** | The timetable for this Procurement as set out in this document. |
| **Supplier or Suppliers** | means a supplier or suppliers (as the case may be) participating in the Procurement |
| **Tender Notice** | means the tender notice with reference NMRNO.2025.008 published on 22nd July 2025 on the Central Digital Platform |

Annex F

Form of Tender

Dear Sir or Madam,

Name of Tender:

I/We, the undersigned, tender and offer to provide the Contract as listed below, which is more particularly referred to in the Provision of IT Security Solutions (2025) supplied to me/us for the purpose of tendering for the provision of the Contract and on the terms of the draft Contract. Included within this document are the following:

Checklist for tenderers

List all documents to be submitted.

| **Document Number** | **Document Name** | **Included (Y/N)** |
| --- | --- | --- |
|  | Appendix D: Tender Response Document |  |
|  | Appendix F: Form of tender |  |
|  | Appendix G: Certificate of non-collusion and non-canvassing |  |
|  | Appendix H: Commercially Sensitive Information |  |
|  | Appendix 1- Security Tender Questionnaire- Completed |  |
|  | <ENTER NAMES OF DOCUMENTS BELOW |  |

**Note:** If Suppliers do not provide all of the items in the checklist, this may result in the response being treated as non-compliant and therefore rejected.

I/We confirm that I/we can supply the contract as specified in our response to the tender requirements and in accordance with the financial model response submitted.

I/We confirm that we accept the terms of the draft Contract as issued with the Invitation to submit for this tender.

I/We understand that the Authority reserves the right to accept or refuse this tender in accordance with the Procurement Act 2023.

I/We confirm that all information supplied to the Authority and forming part of this tender and any previous submissions is true and accurate.

I/We confirm that the Supplier, together with all Associated Suppliers:

• **are registered on the Central Digital Platform**

• **have ensured their information contained on the Central Digital Platform is true and accurate**

I/We confirm and undertake that if any of such information becomes untrue or misleading that I/we shall notify the Authority immediately and update such information should this be required.

I/We confirm that this tender will remain valid for 90 days from the date of this form of tender or until any procurement challenge/s have been resolved.

I/We confirm that I/we are authorised to commit the Supplier to the contractual obligations contained in this tender documentation and the draft Contract.

I/We understand that non-compliance with the requirements of this ITT or with any other instructions given by the Authority may lead to me/us being excluded by the Authority from (further) participation in the Procurement.

I/We agree that the Authority may disclose the Supplier’s information/documentation (submitted to the Authority during this Procurement) more widely within government for the purpose of ensuring effective cross-government procurement processes, including value for money and related purposes.

|  |  |  |
| --- | --- | --- |
| **Signature** |  | |
| **Name (print)** |  | |
| **Position** |  | |
| **Supplier name** |  | |
| **Date** |  |

Annex G

Certificate of Non-Collusion and Non-Canvassing

Statement of non-canvassing

I/we hereby certify that I/we have not canvassed any minister, official, representative or adviser of the Authority in connection with this Procurement and the proposed award of the contract by the Authority, and that no person employed by me/us or acting on my/our behalf, or advising me/us, has done any such act. I/we agree that the Authority may, in consideration of our tender, and in any subsequent actions, rely on the statements made in this certificate.

I/we further hereby undertake that I/we will not canvass any minister, official, representative or adviser of the Authority in connection with the Procurement and/or award of the contract and that no person employed by me/us or acting on my/our behalf, or advising me/us, will do any such act.

Statement of non-collusion

The Authority must receive bona fide competitive tenders from all Suppliers.

In recognition of this requirement, I/we certify that this is a bona fide offer, intended to be competitive and that I/we have not fixed or adjusted the amount of the offer or the price in accordance with any agreement or arrangement with any other person (except any Associated Supplier identified in this offer).

I/we also certify that I/we have not done, and undertake that I/we will not do, at any time during the Procurement or, in the event of my/our final tender being successful, during the term of the contract, any of the following acts:

1. communicate to any person, other than the Authority, the amount or approximate amount of my/our proposed offer except where the disclosure in confidence was essential to obtain insurance premium quotations required for its preparation

2. enter into any agreement or agreements with any other person that they shall refrain from participating in the tendering process carried out by the Authority or as to the amount of any offer submitted by them during the course of this process

3. cause or induce any person to enter into such an agreement as is mentioned in paragraph 2 above or to inform us of the amount or the approximate amount of any other tender for the contract

4. commit any offence under the Bribery Act 2010

5. offer or agree to pay or give or actually pay or give any sum of money, inducement or valuable consideration, directly or indirectly, to any person for doing or having done or having caused to be done in relation to any other tender or proposed tender for the performance of the contract

In this certificate, the word ’person’ includes any person, body or association, corporate or incorporate and ‘agreement’ includes any arrangement whether formal or informal and whether legally binding or not.

I/we agree that the Authority may, in its consideration of the tender and in any subsequent actions, rely on the statements made in this Certificate.

|  |  |  |
| --- | --- | --- |
| **Signature** |  | |
| **Name (print)** |  | |
| **Position** |  | |
| **Supplier name** |  | |
| **Date** |  |

Annex H

Commercially Sensitive Information

*This appendix should be read in conjunction to the PA23 Regulations the NMRN are obligated where applicable to publish a redacted copy of the winning contract, the below is to inform us the areas of your submission to redact from this submission.*

I declare that I wish the following information to be designated as commercially sensitive:

|  |
| --- |
|  |

The reason(s) it is considered that this information should be exempt under FOIA and EIR is:

|  |
| --- |
|  |

The period of time for which it is considered this information should be exempt is:

|  |
| --- |
|  |

Supplier to amend as appropriate [until award of contract OR during the period of the contract OR for a period of [number] years until [month], [year]].

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| **Signature** |  | |
| **Name (print)** |  | |
| **Position** |  | |
| **Supplier name** |  | |
| **Date** |  |