Purchase of IT Software Solutions
Clarifications & Responses Issue 3

	Clarification Question	Responses
1	Annex C refers to the terms and conditions in the bid pack. I cannot locate these please so could you share the terms, or can you advise where they are located.	Please see attached a draft terms and conditions, the NMRN may consider a bidder's own contract including SLAs, please submit this in your submission pack.
2	Also, the document states that submission is via the CDP portal. The tender notice says it is an email submission. Please can you clarify for me, so I am clear how I submit the response to you.	This is an error in the document, all comms and submissions are to come to tenders@nmrn.org.uk email address.
3	Can you please confirm if the current budget that has been provided includes Professional Service and Recurring Revenue? There may be additional costs incurred by NMRN in the delivery in the service (e.g. Licensing costs).	The budget for this tender includes all costs associated with the services, including system licensing costs, SOC costs and any onboarding costs. Please provide a breakdown of costs within your submission.
4	Is there any Azure Servers or Services in use or planned, or those with another public cloud provider?	We have 1 virtual server in Azure. This is detailed in the tender document in Annex A, section 2.
5	If NMRN does have a presence within Azure, can you please confirm the number of subscriptions within your Azure Tenancy?	We currently have 2 subscriptions.
6	Can you advise who your CSP is and if there is any opportunity to change this?	We are not looking to review this at this time.
7	Are your existing M365 Licenses to be considered as part of the bid, or are they expected to remain with the existing provider?	The existing licenses will remain with the existing supplier. Any additional licensing requirements and the cost differences should be included within the proposal.
8	Can you please confirm that you are open to the possibility of adding additional M365 licensing to enable us to provide a service and improve your security tooling, which caters for email and identity security?	Yes, we are open to this possibility.
9	Does NMRN have future plans to migrate on-premise servers to public cloud?	Not at this time.
10	Can you please confirm when you expect the implementation of the service to commence and for the services to go live?	The service should go live by the end of October 2025 at the latest. This is detailed in the tender document within the relevant lots in Annex A.
11	The ITT mentions that a previous tender must be completed prior to the MDR implementation and that any delays to the previous tender will impact this one. Can NMRN confirm that the previous tender work has been completed, or when it is expected to be?	The project following our previous tender is due to be complete by the end of the year, however this will not prevent an MDR service being deployed and we will work with the winning supplier to manage this and provide further details.
12	Can the authority confirm that submissions should be emailed directly to the NMRN tenders mailbox only? 3.2.1 makes mention of a contradictory submission method "via the CDP portal"	See response to Question 2
13	3.1.3 suggests that a pricing proposal should be provided alongside the submission. Can NMRN confirm whether there is a specific or preferred format to this pricing submission?	You are welcome to provide your price response in a format that is suitable to you as a supplier, it must be clear, with a breakdown of all costs and a total price for the Lot(s) you are bidding for.
14	6.2.1 suggests that Tenderers should describe their approach to implementation. Can NMRN confirm where this response should be located and whether this is scored as part of evaluation?	It is linked with the relevant information in Annex A/Scope of Requirements as set out in 6.2.1 which is to then be completed in the Response to Quality Evaluation Criteria for the respective lot(s)
15	6.3.1 suggests that Tenderers should describe the staffing / resourcing to maintain the services on an ongoing basis. Can NMRN confirm where this response should be located and whether this is scored as part of evaluation?	Similar to above it should be stated in the appropriate sections of the evaluation criteria and within the Response to Quality Evaluation Criteria for the respective Lot(s)
16	When responding to Technical Ability (Annex D, Q14), is there a Word Limit to these contract descriptions?	There is not a word limit, however, each of these should be a summary description.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

17	When responding to the requested case study for MDR (Criterion 1, Lot 1, Annex D), is this in addition to the 3 additional requested contract examples within Technical Ability (Annex D, Q14)?	You're welcome to re-use the examples provided in the relevant experiences in 14- Technical Ability and use as an opportunity to expand on these.
18	Can diagrams or appendices be supplied to augment responses to Annex D? Would this be part of the word count?	Diagrams and appendices can be included, however they should not include large chunks of text which would impact the word count.
19	Part of the evaluation, you mentioned a later demo period, can you please confirm what is expected from this demo?	The NMRN would like to see demo's of the platform to better understand features, usability and capability of the service. The full scope of the second stage has not yet been confirmed, but this will be communicated to the suppliers invited to demo in advance.
20	Can you confirm if there is any data residency or classification requirements?	There are no specific classification requirements. Whilst there are also no strict residency requirements, the NMRN would like to understand where data and support services are based and how our data will be used and protected.
21	Is there any compliance or framework requirements for the services?	There are no requirements for this, but if you are compliant with any then please detail this in your submission.
22	Is there any word count limits for the Appendix 1- Security Tender Questionnaire ?	Whilst no specific word count has been included, we are looking for short, concise responses to the criteria.
23	Can you please confirm the location of your servers? on-premise vs Azure and provide a breakdown in each location?	All infrastructure is centralised at our Portsmouth site, with 1 server in Azure. This is detailed in the tender document in Annex A, section 2.
24	Can you please confirm the number of domain controllers that reside within your infrastructure?	2.
25	Can you please confirm the current make and model of your current URL Filtering technology?	We currently use USS from Censornet
26	Can you please confirm the current Email security platform in place?	Darktrace
27	Can you please confirm the current EDR Tool that has been deployed on your Server estate?	We do not have an additional EDR tool in place. Microsoft Defender is deployed across all endpoints and servers.
28	Can you please confirm the current Identity solution in place?	Darktrace
29	Can you please confirm what your current policy state in relation to retaining data within the MDR platform i.e. 12 months or longer?	We have requested a minimum of 90 days but would be happy to see retention of up to 1 year. Logs relating to security incidents may need to be retained for longer or exported.
30	Can you please confirm the current 3rd Parties services that is used for single sign on?	We have Entra Single Sign On configured on a number of SaaS applications, such as Workplace by Meta. We will disclose a full list to the winning supplier, if required.
31	You have mentioned that you have 900 active IP address, to which 400 are accounted for based on your device count. Can you please confirm what the additional 500 IP Addresses are?	The 900 IP addresses is an estimate as we do not truly know how many devices we currently have online. However, other devices would include network equipment, CCTV cameras, access control systems, AV systems and other IoT devices.
32	Can you please confirm that current infrastructure are solely controlled by NMRN or would the chosen supplier be asked to liaise directly or indirectly with 3rd Party suppliers?	The NMRN has a relationship with an MSP who provide additional support to the internal NMRN IT team. It is anticipated that the winning supplier may also need to liaise with them, particularly during incident response scenarios. Unless critical and time sensitive, this would likely be indirectly.
33	Can you confirm the timeline for when the Fortinet firewalls will be replaced with SonicWall?	These will be replaced within the next few months.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

34	Can you confirm the number of firewalls in use and if they are internet facing or not?	There are currently 2 firewalls. They are not currently internet facing and sit behind our ISP's router and firewall. However, this may change in the future and they could be internet facing.
35	You have mentioned that you have 400 End Users devices/Servers. Can you please provide a clear breakdown on Number of end User Devices and number of Servers?	We currently have 346 endpoint devices registered in Intune, plus we will have 17 virtual servers once our current project is complete. There are also a handful of end devices yet to be rolled out, hence the number being estimated at 400.
36	We have some initial clarifying questions to help us gauge whether we can come in within your budget. Could you please supply the below information? • Number of Endpoints • Number of servers • Number of users • Number of email accounts	Please refer to the response for question 35 above. We currently have 228 licensed Microsoft 365 users (all including mailboxes) and an additional 70 shared mailboxes. This is detailed in the tender document in Annex A, section 2.
37	Are there any requirements for the service to hold ISO27001:2022, SOC2 or PCI-DSS accreditations?	Although this is not a strict requirement, we welcome suppliers to disclose if they are compliant with any of these accreditations. There is a question inviting this information within the Appendix 1 questionnaire document.
38	Will products & technologies other than Microsoft Defender for Endpoint be considered if they fully support the Microsoft products currently in the environment?	Yes
39	Can NMRN specify if web filtering is via the SonicWall platform or another solution?	Another solution. Please see question 25 above.
40	Can NMRN disclose what backup solution are used?	Veeam
41	Could you clarify if there is a SIEM or EDR tooling are in place (outside MS Defender suite)?	There is currently no additional SIEM or EDR tooling in place
42	There is mention of zero-day vulnerabilities and resolutions, do you require vulnerability management as part of the service?	No, vulnerability management is already in place.
43	Can you explain your use of Public Cloud – How many Apps/Instances do you have hosted on the Azure Tenant, AWS or GCP?	We have a single server in Azure and we have several enterprise applications registered for SSO and SCIM services. We also have several app registrations in Azure for things like Dynamics 365 and 3rd party app integrations, including 3CX, intranet solutions and a desk booking system.
44	Do you anticipate integrating IoT or OT systems into the security operations in the future?	This is something we would be considering in the future, although we are unable to give an indication of time frame. The focus is on Endpoint and Network for now, but if your solution can provide a degree of protection in these environments through Network Detect and Response solutions, we would welcome the functionality.
45	Are there any future plans to move up to an E3/E5 license?	Not at the moment. However, we are open to the idea of exploring different licensing if there is an added benefit. If your proposal requires E3/E5 licensing, then please detail this in your proposal and detail the cost difference compared to our current 365 Business Premium licensing. We are eligible for Microsoft non-profit licensing.
46	Are there any future plans for a SIEM platform (such as MS Sentinel)? or is NMRN looking for a complete XDR/MDR solution which can provide similar functionality to a SIEM without the variable costs of a SIEM platform?	SIEM is on our radar for the future, however we don't have a definitive timeline for this. If the proposed solution can offer similar functionality to a SIEM across our IT estate, then we are open to this idea.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

47	Are there any requirements for data retention?	Please see the response to question 29 above.
48	Is the desired solution a true 24x7x365 fully staffed Security Service?	Yes. We recognise that some solutions can offer autonomous detect and response actions without the need for human input, and we welcome these solutions. However, we would benefit from the backing of a SOC monitoring the solutions and providing expert security analysis and guidance.
49	**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." We cannot locate an area within Annex D or the Security Questionnaire to respond to these, could you please advise?	Responses will be needed within Criterion 3 for Lot 1 Criterion 3 for Lot 2 Criterion 3 for Lot 3
50	In the CQ's published this morning, Q1 response "Please see attached a draft terms and conditions, the NMRN may consider a bidder's own contract including SLAs, please submit this in your submission pack." We are unable to see this attachment.	To be shared with clarification
51	We noted that NMRN were hit by a Cyber Attack in Dec 2024. Who was the provider that supported you at this time, and what provider continues to offer you support, post recovery?	The NMRN had a pre-existing relationship with an MSP prior to Dec 2024. They provided support during this time and continue to provide support to the internal NMRN IT team to manage the infrastructure.
52	Please can I ask whether it is the expectation of NMRN to utilize the existing Microsoft package as an EDR and SIEM solution? Defender + Sentinel. With that, can I ask what licensing you have for Defender. Ie do you have Defender for Endpoint deployed. Do you have the Defender for Servers added on? Has Sentinel been deployed or in use?	It is not the expectation of the NMRN to use only Microsoft packages, such as Defender and Sentinel, and we welcome other proposals. As detailed in the tender document in Annex A, section 2, we have Microsoft 365 Business Premium licensing which includes Defender for Business. We also have some Defender for Server licenses and Defender has been deployed to all servers. Sentinel has not been deployed and is not in use.
53	Can you provide the draft terms and conditions referenced in your response to Clarification Q1 please?	Please refer to the response for question 50
54	Is it required that all emails to personal email addresses can be flagged or is it just emails to personal addresses that contain potentially dangerous files?	Yes, the solution should be able to flag emails that appear to be sent to personal email addresses regardless of content. This not only helps to identify

		malicious files but will help to identify potential data loss incidents.
55	Do NMRN need detailed inspection of emails for 90 days or just logs of what happened or triggered a security policy?	Log summaries will be sufficient here to identify what triggered a security policy and what actions were taken against the email. Detailed inspections should be possible for recent email traffic.
56	Does the NMRN envisage the MDR service including the same Microsoft technology, and for that licence cost to be included in the stated costs for the service?	It is not the expectation of the NMRN to use only Microsoft technologies as part of the MDR service. We welcome solutions from any reputable vendor. However, if Microsoft packages are being proposed, any required licensing costs should be included within the proposal.
57	Can NMRN please expand on what it requires/expects from the 'Forensic investigation' requirement in Lot 1?	The NMRN would expect the forensic investigation to take place post-incident to help identify the origin and nature of the threat/attack, and determine the potential impact of the attack, such as identifying lateral movements by the attackers to pinpoint services/data that was targeted.
58	Can you please confirm are you expecting the chosen supplier to integrate USS from Censornet into the MDR Solution?	No, this is not a requirement.
59	You have mentioned that your Servers are protected by Defender, can you please confirm if this Defender for Cloud Server plan 1 or plan 2?	Our Servers are on-premise, with the exception of the single server in Azure. We have Microsoft Defender for Endpoint Server in place on all of these.
60	You have mentioned that you have CCTV cameras, access control systems, AV systems and other IoT devices, to counts towards the additional 500 devices. Can you confirm if you have Defender for IoT in place?	No, we do not have Defender for IoT in place.
61	Can you please confirm the service that the current MSP provides?	The MSP provide several services to the museum including 3rd line IT support services, cyber security guidance and services, IT strategy guidance, professional services and project support.
62	Will the new Sonicwall Firewalls be configured with IDS/IPS?	Yes, they will include SonicWall's Advanced Protection Service Suite.
63	Considering the overlapping services of the 3 proposed lots, it would be difficult to split this into a per-lot pricing model. Would NMRN consider a single pricing model, covering all 3 lots?	As stated in the tender document in Annex A, section 3, we welcome bids across multiple lots and encourage you to detail the benefits of implementing a unified platform within your response. Pricing proposals need to remain within the budget limits set out in the ITT, however pricing for each lot should be visible for a fair comparison between suppliers.
64	The documentation mentions that hybrid working is possible. Could you kindly confirm whether service provision from outside the UK (e.g., offshore delivery from India) would be acceptable?	Services should be compliant with UK GDPR and data protection laws to ensure the safety of NMRN data. A main point of contact within the UK would be preferred but the service can be delivered from multiple worldwide locations. Please disclose the locations of the teams delivering the service within your response.
65	Are there any specific requirements related to UK citizenship, UK residency, or baseline/security clearance for personnel involved in delivery?	No, this is not a specific requirement.
66	Could you also please confirm whether we are required to submit: Three references **for each lot** we are bidding for, or • Three references **in total**, with one reference covering each lot?	Three references in total will be fine if you are bidding in multiple lots.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

67	Would the solution need to automatically determine if the recipient was a personal email address, or would a list of domains used by personal email addresses that is manually built and maintained by the customer be sufficient?	Ideally the solution should be able to determine is a recipient was likely to be a personal email address of the sender, to dynamically detect potential data loss incidents. However, we are open to other solutions so please detail your approach in your response.
68	Could you inform us if this opportunity is open to International Bidders? We are registered in the USA.	Yes, international bidders are welcome. However, services should be compliant with UK GDPR and data protection laws to ensure the safety of NMRN data.
69	How many servers are currently deployed in your cloud and on-premises environments?	Please see the response to question 35 above and details within the tender document in Annex A, section 2.
70	Are all deployed servers currently licensed for XDR coverage?	No, we do not have XDR in place currently.
71	Can you please provide the total number of endpoints in your environment?	Please refer to questions 35 and 36 above, as well as details within the tender document in Annex A, section 2.
72	How many cloud resources are currently in use within your environment?	Please refer to previous questions throughout this document, including 9, 23, 43. Please also see the tender document, Annex A, section 2.
73	Is a SIEM (Security Information and Event Management) currently configured and actively used in your environment?	No, please see responses to questions 41 and 46.
74	Should SIEM ingestion costs be included in our pricing proposal?	This is not required as we do not have a SIEM currently in place, however it may be useful to understand for future reference if you wanted to include this within your submission.
75	What is the required retention period for log data within your SIEM solution?	N/A
76	Are there any network security devices in use beyond Fortinet and SonicWall appliances?	Internally, no. Our ISP provide a router and firewall service separately, however.
77	How many non-user endpoints (e.g., kiosks, digital signage) are present on-site that require coverage?	At this time, there are no additional non-user endpoints within scope of the NMRN's internal networks. It is envisaged that any additional devices such as this would be monitored by the Network Detect and Respond piece, however we would be happy to discuss this further with the winning supplier.
78	Are the non-user endpoints currently licensed with Microsoft Defender for Endpoint?	No
79	Do you currently have a Critical Incident Response (CIR) provider under contract?	No

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

80	Is it a requirement for SOC analysts to be based in the UK?	Please see the response to question 64 above. Suppliers are invited to provide the locations of their teams providing the service within the Appendix 1 questionnaire document.
81	If the bidder proposes Microsoft technology to provide any of the functionality, for example maybe the "Defender for Identity" and/or the "Defender for 365" bolt-ons, is it expected that these (as well as any other underlying EDR, XDR, NDR) license costs are included within the response as part of the max available budget costs for each lot?	Yes, additional licensing costs will be included in the maximum available budget.
82	If any Microsoft licensing costing is to be included in the budget by the bidder, can the winning bidder be expected to provide NMRM the licenses for these components under a new CSP agreement, or do you have an existing CSP partner you would use or even an EA?	We do have an existing CSP partner. Additional licenses could be purchased either through the existing partner for ease, or we could look to purchase under a new agreement if required.
83	If Microsoft licensing costs are to be included in the budget, do you currently qualify for charity pricing with your charity number?	Yes, we do qualify for charity licensing. Our existing Microsoft licensing is purchased at non-profit rates.
84	In Annex A-2. It is mentioned that the 365 services used by MNRN include Teams/SharePoint/OneDrive alongside some endpoint, email, and identity capabilities, including managed detection and response, required for Teams/SharePoint/OneDrive, endpoints, email, and identity. Typically these would fall under MXDR (Managed eXtended Detection and Response) banner.	Annex A, section 2 details our current infrastructure status and existing security solutions. Lot 1 – MDR focusses on managed detection and response across endpoint and network. The MDR service is not required to cover Lots 2 and 3. Lot 2 – Email focusses on an email security solution. Lot 3 – Identity focusses on an identity security solution which will monitor and protect our Microsoft accounts across 365 services.
85	In Section 3.2 of your ITT you state that responses can be emailed to tenders@nmrn.org.uk however in section 3.2.1 you state that bidders ITT and Supporting Documentation must be submitted via the CDP and that "Hard copy, paper or delivered digital Tenders (e.g. email, DVD) are no longer required". Not only are these 2 statements contradictory, but the CDP is not for suppliers to upload bid response documentation on specific contracts. The CDP is for suppliers to share their company information (annual accounts, certificates, persons of control etc) via a Share Code and CDP download file. There is no facility for bidders to use the CDP in the way you have instructed. Please can you confirm therefore that the correct method of bid submission is by email to the given address, and please confirm that there is no portal being used for the submission of ITT information.	All bids must be submitted to tenders@nmrn.org.uk before the stated deadline. To ensure your documents are received it is recommended to email and express your interest in this tender in advance. To understand who the NMRN are please see www.nmrn.org.uk
86	Is it expected that if the supplier is to propose the use of your Sentinel License as a SIEM tool, the cost of ingestion would need to be factored into the quote? Please can I ask what the expected Ingestion per day is expected to be? – in order to provide a cost for sentinel ingestion costs we would need this information. Eg 5GB/Day	We do not have Sentinel licenses and SIEM is not a requirement of this tender. Please see responses to questions 41 and 46. All costs associated with the proposed services need to be factored into the quote.
87	The ITT references using 365 for Email security and Identity security. Can you please confirm what services/licenses are currently being used to deliver this?	We are not suggesting Microsoft 365 tools need to be used for email and identity security. The security solutions will need to support 365, as we use Microsoft 365 services across the business.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

88	Can you please confirm if there is a managed service applied on top of the 365 Email and ID security?	No, we do not require a managed service on top of the email and identity pieces. If you are bidding on multiple lots and would be offering a service which provided this coverage across all three lots, please detail this in your response. We would be happy to consider this.
89	Can you please confirm if the renewal date applies to the managed service or the licenses?	The expiry date for our existing services only applies to the email and identity solutions currently in place.
90	Can you please confirm the impact of not meeting the target live date for each lot as the timeframe from project start to live date is limited.	The impact of not meeting the email and identity solution dates would be significant as this would leave a gap in our existing defences. The MDR piece is less critical as this is a new service, however we are keen for this to go live as soon as possible and would be aiming for this to go live towards the end of October with the email and identity solutions.
91	What operational contingencies have NRNM put in place for the delivery date if the contract award date is not met? Are these backed by your contract with the incumbent?	The existing services for email and identity expire on the 31st October 2025 as detailed in the tender document. There is no extension to these contracts. New services will need to go live to take over from these services.
92	Can NRNM please confirm who the incumbent supplier is for the services in lots 2 and 3?	Please see responses to questions 26 and 28.
93	Can you please confirm your current notice period with your incumbent supplier?	Contracts expire on the 31st October 2025 as detailed in Annex A of the tender document.
94	Can you please confirm what resources are available to NRNM to ensure delivery is made on-time.	Suppliers would be working with the internal NMRN IT team to implement solutions. It is anticipated that the winning supplier would assist with the deployment of the solution.
95	The timeframe from ITT submission to contract award is short when considering the complexity of the ITT. What plans have been put in place for scoring the ITT and comparing the solution against ITT requirements?	Please refer to Section 5 of the ITT document
96	Can you please confirm why the services have been separated into 3 lots?	Not all suppliers offer all 3 solutions, so we wanted to ensure we reach as much of the market as possible.
97	NRNM mention their existing MSP 'ROCK IT'. please confirm if you are referring to: ROCK | IT Consultancy Services or Rock IT | Business IT Support	We have an existing relationship with an MSP, ROCK IT Specialists Ltd.
98	Lot 1 Criterion 4 & 5, Lot 2 Criterion 2 & 3, Lot 3 Criterions 2 & 3 reference 'Sections' within Annex A that cannot be found. These criterions also seem to overlap in content /requirements. Can NRNM confirm how these criteria should be responded to?	Within Annex A, there are numbered headings. Sections 4/5/6 refer to the individual lots. Please refer to the correct section based on these headings. Please response to each criterion independently.
99	Can you please confirm the number of Firewalls in place	2
100	Can you please confirm what element of 'security awareness training' (annex A, section 2), that bidders would be expected to pick up. Please details type of training, topics, number of users, in person/virtual etc. If this is not expected to make up part of the bid please confirm.	This is not required. Annex A, section 2 details the current security measures in use by the NMRN.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

101	As part of the submission, can we provide an appendix to inform the NRNM on our organisational credentials and expereince in providing services to similar not-for-profit orgnaisations?	You are welcome to supply this, but please note this does not form part of the evaluation scoring process. Within the response, you are also required to submit some reference contracts under Annex D. The criteria for lot 1 also requires a case study from a previous solution deployment.
102	Can a copy of the draft contract Terms and Conditions, mentioned in the previous round of CQs please be provided to each bidder?	There were shared with the previous clarification questions issue and are also available on the tender advert online: Provision of IT Security Solutions (2025) - Find a Tender
103	What would be deemed a critical risk(s) to the ongoing operations of NMRN based on your current environment and business operations?	The NMRN is currently undergoing an infrastructure refresh to implement new and appropriately scaled solutions to support operations for the next 5-7 years. This includes backup and DR solutions. Therefore, it feels as though cyber risk is the biggest risk to the ongoing operations of the NMRN at the moment. Attacks in the sector are on the rise, and we need to be appropriately prepared for further incidents to occur.
104	What are the driving factors for this particular project?	Please refer to Annex A, section 1 in the tender document. The NMRN also suffered a cyber-attack in December 2024 so are looking to increase security measures moving forwards.
105	How is your current security set-up impacting on these goals?	We have gaps in our existing security solutions that do not give us the correct levels of visibility within our environment, nor the desired level of threat response.
106	Where does security (and by extension this project) fit into NMRN's wider digital transformation roadmap?	Whilst the NMRN does not have a dedicated digital transformation roadmap or strategy, cyber security needs to be at the forefront of all we do moving forwards to ensure we provide secure foundations to continue to operate securely in an increasingly digital world. This has been agreed within the business and cyber security will continue to be invested in and develop so that we stay up to date with new and emerging threats.
107	Would you consider amendments to your existing Microsoft license footprint as part of this project, to access additional security feature sets?	Yes
108	Is security awareness training provided internally or via a third-party platform?	We use a third-party platform to deliver the training, but this is managed by the internal IT team.
109	Do you currently have access to an Incident Response provider in the event of an attack/breach scenario?	We would work with our MSP in this scenario.
110	Regarding your server estate, how many of the following resources are in place: - Web servers - Database servers - DHCP Servers - DNS Servers - Email Servers	Currently: - Web servers - 3 - Database servers - 4 - DHCP Servers - 2 - DNS Servers - 2 - Email Servers - 0 - Domain Controllers - 2 - Web/Mail Gateways - 0

	- Domain Controllers - Web/Mail Gateways	
111	Are any of your servers virtualised? If so, what hypervisors are in use?	All servers are virtualised. This is currently being configured in Hyper-V.
112	Are there plans to migrate your on-premises resources into the cloud?	Please see response to question 9.
113	How many network switches and routers do you have deployed?	Across all 6 NMRN sites: Routers – 6 production/main line routers, 6 backup line routers. Switches – 38
114	What other network devices do you currently utilise?	Network devices include routers, firewalls, switches and wireless APs.
115	How many Firewalls will you have once the new SonicWall deployments are in place, and what configuration will they be in (e.g., HA pairs)?	2, in a HA pair.
116	How many IDS/IPS devices do you have deployed?	We have IDS/IPS on the firewalls.
117	Is there a vulnerability management solution in place?	Yes
118	How many VPN devices do you have deployed?	We utilise the Azure VPN, and all user endpoints are able to connect to this.
119	How many wireless access points are there across your 6 sites?	113
120	Do you enforce data classification and DLP?	Not currently.
121	What standards or regulations does NMRN currently/aim to comply with (e.g., ISO27001, Cyber Essentials etc.)?	We are working towards Cyber Essentials, with an aspiration to achieve CE+ in the future.
122	Do you utilise any third parties or MSPs to provide IT support?	Yes, please see the response to question 97.
123	How are BYOD devices currently managed?	BYOD can only be used to access Microsoft 365 services online. Access to these services are regulated by conditional access policies. BYOD cannot be used internally on the NMRN's network.
124	Do you have any ICS/OT/SCADA systems on your network?	We have a few BMS systems and one example of a SCADA system monitoring load cells, however these systems are currently disconnected from our network.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

125	Are there any key third-party apps that your users' access?	There are some products that teams use, such as Adobe suites and Autodesk products. We also have a number of third-party apps configured for Entra SSO. We would be happy to discuss this more with the winning supplier, if required.
126	Could you please confirm the amount of end points and servers?	Please see the response to question 35 and refer to Annex A, section 2 in the tender document.
127	The Email Security requirements state "the system must integrate with training solutions". Do you have an existing Security Awareness training solution you prefer to integrate with? Can you please define if you require native integration or are you looking for the Email solution to simply be able to inform and assist this?	The email security solution should be able to be informed of and assist the training solution so that it does not prevent the delivery of training material or phishing campaigns.
128	Are you open for a solution to include a training solution as part of the offering?	We are not currently looking for a training solution, however if it is built into the platform being proposed and would be available as part of the service, we would be open to this.
129	We'd like to know how many users will be using the below services. ***Lot 1. Managed Detect and Response (MDR)*** ***Lot 2. Email Security Solution*** ***Lot 3. Microsoft 365 Identity Security Solution***	Please refer to Annex A, section 2 in the tender document for device and user numbers.
130	Given that NMRN already uses a URL content filtering solution, is there an expectation for the MDR provider to replace this functionality, or can the existing solution be leveraged as part of the overall security stack?	This is not a core expectation of the MDR service, however the NMRN recognises that some providers may offer this within their solution, so we have invited this detail. The existing solution will continue to be used as part of the overall stack if this functionality is not within the winning MDR service.
131	Is there a current vendor providing services under Lot 1 – Managed Detection and Response (MDR), and do you anticipate them submitting a response to this RFP?	No, as detailed in Annex A of the tender document, the NMRN does not currently have an MDR service in place.
132	Could you provide an estimate of the average number of security alerts generated monthly by your existing security tools?	The security tools that currently generate alerts are Microsoft Defender, plus the email and identity security solution.
133	What is the anticipated monthly log volume (in gigabytes) expected to be ingested by the SIEM platform?	SIEM platforms are not a requirement of this tender.
134	To properly scope efforts related to encrypted traffic analysis, could you share an approximate monthly volume of firewall traffic (in gigabytes)?	We do not have this information to hand for all sites as the edge firewalls are dealt with by the ISP. We will work with suppliers to provide this information as required as this process progresses.
135	Are monitoring services permitted to be delivered by EU-based resources, provided that no data leaves your environment? Or is a UK-based provider specifically required?	This is fine. Services should be compliant with UK GDPR and data protection laws to ensure the safety of NMRN data. A main point of contact within the UK would be preferred but the service can be delivered from multiple worldwide locations. Please disclose the locations of the teams delivering the service within your response.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

136	Is there a preference for the Extended Detection and Response (XDR) platform to be deployed on-premises, or are cloud-hosted solutions acceptable?	Either deployment method is fine. Please detail this in your response.
137	Are we able to include screenshots/images within our responses to demonstrate and evidence our responses?	Yes, please refer to the response to question 18.
138	Could you clarify if there is any weighting aligned to the MDR case study being in the UK or International that we submit or is there no particular preference as we have both.	There is no particular preference to this, however we would encourage suppliers to offer the most relevant case study available.
139	Do you require to have Cloud, SaaS and OT environments detected within the same platform?	Whilst cloud, SaaS and OT security is not an immediate requirement, it is a future consideration which is why it has been referenced in the questionnaire document. If we were to expand into cloud, SaaS and OT security in the future, we would anticipate this being dealt with by the same platform.
140	What is your current, or planned roadmap for Cloud Adoption, including which Cloud Service Providers?	There is no current plan to migrate additional systems to the cloud. If this changed, it would likely be using Azure or possibly AWS.
141	Do you need a single platform to provide response actions across Endpoint Protection, Identity Security and Email Security	Not necessarily, which is why they have been split into individual lots. However, the NMRN recognise that this can provide additional security benefits and a holistic view of threats. As referenced in Annex A, section 3 within the tender document, please detail this and the benefits in your response if you intend to bid on all 3 lots. Please note, lot 1 MDR focusses on endpoint and network security.
142	Do you require your Cyber Essentials to cover the entire solution platform?	The NMRN are working towards Cyber Essentials compliance across the entire IT estate so we anticipate the security solutions assisting in this, even though they may not be direct requirements for compliance. We have encouraged suppliers to disclose whether they are also compliant with Cyber Essentials within their response.
143	Do you require ISO27001 to be latest, ISO27001:2022?	This is not a critical requirement but please detail what accreditations you have within your submission. This is invited in the Appendix 1 questionnaire document.
144	Do you also require 24x7 human-led threat hunting service?	The scope requires 24/7/365 threat monitoring, plus active threat hunting. Please detail the frequency of threat hunting proposed within the service in your response.
145	Is it permissible to submit a combined commercial response for Lots 1 and 3, with a total cost of £200,000, aligning with the individual budgets of £180,000 for Lot 1 and £20,000 for Lot 3. Specifically, can we present a unified pricing structure that covers both lots, rather than submitting separate commercial breakdowns for each?	Please see response to question 63.
146	Are all your existing 228 M365 licenses M365 Business Premium or do you have a mix e.g. M365 E3 or E5? If so, what is the split?	They are all 365 Business Premium.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

147	Have you purchased any Microsoft Security Add-ons to complement the above licencing	Only Defender for Endpoint Server licenses.
148	Do you have any central logging for security or system events in place?	No
149	Out of the roughly 400 devices, what is the split between Windows 11 and Windows Server (22/25)?	All endpoints are Windows 11 (currently 346 registered in Intune). All servers (17) will be WIndows server 2025 with the exception of 3, which will remain on 2022 for now.
150	Can you describe your LANs - which switches, access points are in use? Is there a standardised design?	We use Aruba CX switches across the LAN and Unifi APs. Our core switches are Aruba 3810M switches.
151	Can you confirm that you have on-premises Windows servers or are they all cloud-based (IaaS)?	All on-premise, apart from 1 server in Azure.
152	How are security alerts handled currently?	Alerts are monitored through the 365 Defender portal, some are emailed to the IT team and other solutions in place also have mobile apps which notify the IT team on their devices.
153	Do you have a willingness to use core Microsoft Services augmented by the Managed Service Provider to provide a fully compliant bid?	We are open to this idea.
154	Will the successful bidder be responsible for supplying Microsoft licences where they form part of the solution, or would this be done by the incumbent? If supplying, should these been shown in total cost	Any additional licenses required can be supplied by the winning supplier, or our current licensing provider. We are happy to discuss this with the winning supplier. Please note, there is no incumbent supplier for our current Microsoft licensing. Any additional licensing required as part of the solution should be included in the total cost, regardless of where it is eventually purchased from.
155	Does the SOC expect to take calls from end users, or from NMRMs service desk	No, they will likely only communicate with the NMRN's IT team and potentially our MSP in a threat situation.
156	What are times of NMRM's business operations	Teams are onsite working from around 7am-6pm, however we often hold events on our sites outside of these hours and have an online presence with websites and online stores etc. 24/7.
157	What is your existing EPP/EDR/AV solution	Please refer to the tender document, Annex A, section 2.
158	What out of hours IT support does NMRM have	The IT team currently work core office hours (Mon-Fri, 9-5), but are on-call for emergencies out of these hours. The MSP we work with provides a degree of 24/7 coverage and infrastructure resource monitoring.
159	Can you please list any key devices (quantity, type and role/function) that you feel would provide important log sources for the security service	At the moment, this would likely be the switches, routers, firewalls, servers and endpoint devices across the network. Quantities are detailed in Annex A, section 2 of the tender document and previous clarification questions.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

160	Please advise the type and level of licencing deployed for: • MS Defender (endpoint, identity, office 365 etc) • E5 security (if applicable) • Entra ID plan level	Microsoft Defender for Business (included within 365 Business Premium licensing) Microsoft Entra ID P1
161	Is any Data Sensitivity marking in place, or required?	It is not currently in place and is not a direct requirement of this tender, however we would consider it on SharePoint etc. Please detail this in your response if you propose this.
162	Please describe the server estate (location -ie cloud/DC, any hypervisor, roles of servers, OS's installed etc)	Please refer to the tender document, Annex A, section 2. Roles of servers and hypervisors used are detailed in previous clarification questions.
163	Is the log retention requirements (90 days) the same across all lots?	Log retention requirements are detailed in the relevant lot scopes in Annex A of the tender document.
164	In regards to Licensing Questions. How many servers are in the NMRN environment? The document mentions 400 devices total. 346 endpoints shown in Intune, 17 virtual servers + 1 server in Azure is 18 servers accurate?	The 17 servers includes the Azure VM.
165	Regarding the six sites identified in the RFP: • Does each site have its own direct internet access or is internet fed via VPN from one or more sites? • What is the internet bandwidth at each site? • Approximately how many of the 228 users reside at each site? • What switching technology and connectivity (10Gb Fibre, copper, etc) is used?	- Each site has it's own internet connection and the MPLS is provided by the ISP. - We have sites with 100Mbps, 200Mbps and 500Mbps. This is likely to increase in the future. - Portsmouth has the most, with around 150 users. The Fleet Air Arm has around 30, the Submarine Museum, Explosion and Belfast have around 10 each and Hartlepool has around 15.
166	In Lot 3, do you please have any detail around the current licence types deployed?	Our current 365 licesning is available in Annex A, Section 2 of the tender document. The existing identity security solution is not a Microsoft solution.
167	What is the Primary Identity Provider (e.g Entra ID / AD)?	AD
168	What is the Secondary Identity Provider (e.g Entra ID / AD)?	Entra
169	If Entra is used do you know if it is Plan 1 or Plan 2?	P1
170	Is Defender for Office or Cloud apps used?	No
171	Which MFA technology is used (e.g Microsoft, Duo, Okta)?	Microsoft
172	Which Wireless Access points are used (e.g Meraki, Ubiquiti)?	Ubiquiti Unifi

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

173	Are any SSE devices (e.g Zscaler, Cato, Netskope)?	No, just the firewalls described in Annex A, section 2 of the tender document.
174	Are any proxy technologies used (e.g Zscaler, ProxySG, Citrix)?	No
175	Which DNS is utilised (e.g Active Directory, Cisco Umbrella)?	AD for internal networks only. Other isolated networks use public DNS.
176	Does NMRN have any kind of Intrusion Detection Systems (IDS) monitoring traffic?	No, although the new SonicWall firewalls will include their APSS licensing.
177	Does NMRN have any Cloud Security Posture Management (CSPM) tools in place?	No
178	Is Google Workspace, Box or SFDC used? If so - please detail.	No
179	Does the NMRN have any service for dark web scanning of leaked RFU employee credentials?	No
180	Does NMRN have regular scans of any public facing environments or penetration testing?	Yes
181	What Security Frameworks does NMRN follow, if any (e.g. CIS, NIST, CE+)? or is there desire to align to a particular framework?	Currently working towards CE
182	If we are bidding for Lot 1 only but possess overlapping capabilities relevant to Lots 2 and 3, would it be acceptable to briefly complete some the relevant sections of Appendix 1 for Lots 2 and 3 to demonstrate our integration capabilities? Or would you prefer that vendors confine their responses strictly to their chosen Lot and outline any cross-Lot integration within the lot they are bidding for?	It would be preferable to only respond to the Lots you are specifically bidding for. Please put any additional insights that may overlap into your specific Lot submission as additional information.
183	Can you confirm the expected response layout? Is it permissible to submit a traditional tender document with the Quality Evaluation Criteria pasted somewhere inside or do you only want your tender document, the QEC + Appendix 1 at this stage.	You are welcome to use the ITT forms as set out in the tender document. This should be completed from Annex D all the way through with all forms and signatures completed. With Appendix 1 completed and submitted for the relevant lots you are bidding If you wish to submit your written response on an alternative format you are welcome to, however, it MUST clearly show the Lot and questions clearly. Failure to do may result in zero scores given. Price breakdowns should be submitted with clear total bid price for your proposal visible.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

184	What are key deployment considerations for Darktrace identity and email solutions rather than Microsoft – is it due to license or operating system or other reasons?	The Darktrace solution was implemented at the time as it offered enhanced security detection, automated responses and threat containment, and very little user configuration was required.
185	Is Power BI licensed for all users?	No
186	Would a phased or partial upgrade (e.g., for privileged users or sensitive groups) be considered acceptable?	We are looking at implementing these solutions across the entire business rather than in phases.
187	Is Incident Response and operational performance of Microsoft Defender expected to fall within the MDR provider's scope?	If the MDR service is proposed to use Microsoft Defender as the EDR tool, then yes. The MDR provider would be expected to provide the incident response capability and ensure the solution they proposed was optimised for best results.
188	Of the approximately 400 devices, can you confirm the split across: • Windows endpoints • Windows servers • Mobile devices (iOS/Android) • macOS or Linux devices	Please see previous clarification responses.
189	Are mobile devices (iOS/Android) expected to be in scope for endpoint protection and MDR monitoring?	No
190	Are any macOS or Linux devices part of the estate? If so, how are these currently secured?	No
191	Are all endpoints currently enrolled and compliant in Microsoft Intune?	Yes. Some devices may fall out of compliance from time to time due to inactivity, but these are updated to compliance levels once online.
192	Is the MDR provider expected to take responsibility for managing device policies and profiles via Intune?	No, unless this is required to deploy the the proposed service and maintain security standards.
193	What email and identity security platforms are currently in use (e.g., Microsoft Defender for Office 365, Darktrace)?	Please refer to questions 26 and 28.
194	Are these expected to be retained, replaced, or run in parallel with the MDR solution?	If this question is referring to the email and identity solutions, then these solutions are also out to tender due to contract expiry. They are detailed within the document under lots 2 and 3. We require a solution for all 3 lots.
195	Is NMRN seeking an ongoing managed service for email and identity protection platforms (e.g., Microsoft Defender for Identity, MDO)?	Please refer to question 88.
196	Alternatively, is the MDR provider only expected to ingest logs from these platforms?	We have not set firm expectations around what logs the MDR solution should ingest. Please detail what you would expect and recommend to be ingested in your submission.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

197	What is the rationale for running both Microsoft Defender and Darktrace for email and identity protection? • (e.g., platform gaps, resilience, specific feature sets)	We currently only run Darktrace as our email and identity security tools.
198	Is NMRN open to consolidating these controls under a unified solution such as Microsoft XDR?	We are open to the idea.
199	Is the MDR provider expected to: • Provide threat notification only? • Isolate compromised endpoints? • Undertake full remediation and recovery actions?	Please refer to Annex A of the tender document for the Lot 1 – MDR requirements.
200	In the event of a security incident, what is the delineation of responsibilities between the internal IT team and the MDR provider?	Please refer to Annex A of the tender document for the Lot 1 – MDR requirements.
201	Who will be responsible for restoring infected endpoints to a known-good state (e.g., backups, rebuilds)? Internal IT or the MDR provider?	This would likely be the internal IT team, but please detail your recommendations in your response. We will work with the winning supplier to determine this.
202	What secure remote access mechanisms are permitted for MDR personnel (e.g., VPN, SSH, Azure VPN)?	The NMRN would like to the MDR provider to propose a preferred method as part of the response. This information is invited in the Appendix 1 questionnaire document.
203	Will MDR analysts be granted secure access to NMRN's Azure environment?	If required, yes.
204	Will access to managed NMRN endpoints be enabled via Azure VPN or another access method?	Please refer to question 202.
205	What is the rationale for upgrading from Fortinet (1 Gbps) to SonicWall NSA4700 (>9 Gbps)?	The Forigate devices are due to be replaced as they have been in place for some time. The SonicWalls have been scoped to meet current and future requirements.
206	Are additional firewall capabilities anticipated (e.g., SD-WAN, application identification, IoT protection)?	It is likely the NMRN will move towards SD-WAN in the future and will also look to integrate things like IoT security as security systems develop as well.
207	Are firewall logs expected to be ingested into the MDR/XDR platform?	This information is invited within the response documentation. Please detail what you recommend to be ingested into the platform in your response.
208	Why is URL filtering handled by Censornet USS rather than the firewall feature?	USS was in place prior to the licensed firewall feature and it offers more granular control based on the user account.
209	Do you have estimates for daily/monthly log ingestion volumes (in GB) for each source?	No, we do not currently have this information.
210	If existing tooling (e.g., Darktrace) is being phased out, will log access remain available throughout the transition?	We could look to export any logs from current solutions as required.
211	Could any existing supplier involvement impact or create dependencies for this MDR contract?	Not that we are aware of.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

212	Should the MDR solution provide full monitoring of Identity Security systems (e.g., Defender for Identity)?	Please refer to question 88.
213	If yes, should this include domain controllers, Entra ID, and other identity-related infrastructure?	Domain controller servers should be monitored by the MDR service as part of the endpoint security.
214	Will NMRN pay annually and the customer pays us annually or will they paying for the full 3 years in advance?	Annually.
215	In the "Response to Quality Evaluation Criteria" Section in Lot 2 Email Security Solution, Criterion 3, the question presented is as follows: *"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?"* However there does not appear to be an Annex A, Section 5 visible in the document?	Section 5 refers to the Lot 2 – Email Security Solution scope.
216	Likewise, In the "Response to Quality Evaluation Criteria" Section in Lot 3 – Microsoft 365 Identity Security solution, Criterion 3 the question presented is as follow: *"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?"* However there does not appear to be an Annex A, Section 6 visible in the document?	Section 6 refers to the Lot 3 – Identity Security Solution scope.
217	Would it be acceptable to propose a SIEM solution as part of our offering, if it was to fit commercially?	SIEM is not a requirement of this tender. However, if the proposed solution requires one then please detail this in your response and include all costings.
218	Can we confirm if this is 24/7 eyes on glass requirement?	Yes, the Lot 1 – MDR service requires 24/7/365 threat monitoring.
219	Can you clarify how log ingestion is being handled and the methods or tools being used?	We don't currently have any tools in place to ingest logs.
220	In regard to the IT Security Solutions opportunity are there any personnel or vetting checks required for the resources who will perform the work?	Please refer to questions 64 and 65.
221	Is there an appetite from NMRN to purchase additional Microsoft Licensing, such as Purview?	We are open to the idea. If this is a requirement of your proposed service, please provide details within your submission and include all additional licensing costs.
222	Is there an appetite from NMRN to Microsoft Sentinel subscriptions, analytics and logging?	We are open to the idea, however, please note that SIEM is not a requirement of this tender. If this is a requirement of your proposed service, please provide details within your submission and include all additional licensing costs.

Purchase of IT Software Solutions
Clarifications & Responses Issue 3

223	For all Questions after page 28 that refer to Annex A, Section X, what exactly are these questions referring to? For example, under Lot 3- Microsoft 365 Identity Security Solution, criterion 3 there is a reference to Annex A, Section 6 – but Annex A (starting on page 15) does not seem to have a section 6.	Annex A, section 4 refers to Lot 1 – MDR Annex A, section 5 refers to Lot 2 – Email Security Annex A, section 6 refers to Lot 3 – Identity Security

- **Submission Deadline for this tender is Midday Monday 18th August 2025**
- **All submissions are to be sent to tenders@nmrn.org.uk**