

	Tender Questions and Answers	Document Identifier	240-7124948	Rev	1
		Effective Date	01 July 2024		
		Review Date	July 2027		

TENDER CLARIFICATION –

DESIGN, SUPPLY, DELIVERY, INSTALLATION, COMMISSIONING, MAINTENANCE, SUPPORT AND TRAINING OF AN OPERATIONAL TECHNOLOGY (OT) SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION FOR A PERIOD OF FIVE (5) YEARS

Request Number: 01	Request for Quotation (RFQ) No.
Date issued: 01/07/2026	E2024NTCSAMWPR

The following clarification is needed in response to queries and questions raised by Tenderers.

Questions in **BLUE** and Answers in **BLACK**

Number	Clarification / Discussion
Q1	We are currently preparing our proposal for the Operational Technology (OT) Security Information and Event Management (SIEM) solution tender. To ensure our technical architecture and commercial pricing align exactly with your infrastructure requirements, please kindly provide clarification on the following points: 1. Archive Storage Requirements • Is there a specific archive storage technology, medium, or retention period that NTCSA requires for this solution? • Alternatively, should bidders propose an independent, self-contained archiving sub-system as part of the software architecture? 2. Daily Data Volume • What is the current or projected daily data volume (e.g., in Gigabytes per day or Events Per Second / EPS) that the SIEM solution must be sized to ingest and process? 3. Load Balancing Infrastructure • If the proposed architecture requires load balancing, does NTCSA provide a shared enterprise load balancer solution for vendors to leverage? • If no shared infrastructure exists, must the cost of dedicated load balancers be included directly within the bidder's solution pricing? 4. Regional Collector Servers • Should the pricing for the Regional Collector servers be included in the bidder's financial proposal? • Alternatively, will NTCSA provision and provide the underlying hardware/virtual machine environments for these regional nodes? We appreciate your guidance on these technical specifications to help us submit a highly accurate and competitive proposal.

	Tender Questions and Answers	Document Identifier	240-7124948	Rev	1
		Effective Date	01 July 2024		
		Review Date	July 2027		

Number	Clarification / Discussion
A1	- Archive Storage Requirements - Data retention strategy is specified in section 3.2.6 of doc no: 240-185000083. - Yes, bidders can propose an independent, self-contained archiving sub-system as part of the software architecture to ensure the requirement in 3.2.6 of doc no: 240-185000083 are met. - Daily Data Volume - For tendering purpose, assume that the ingestion rate is 200-300 GB/day. The supplier should indicate if they have tools to estimate the ingestion rate. - Load Balancing Infrastructure - No load balancing infrastructure exist for the supplier to leverage on. However for the two systems that require Active-Active operation, the supplier should ensure that dependencies for this mode of operation form part of their offering. - Regional Collector Servers - The solution is expected to have no external dependencies. All components of the solution should be provided as part of the proposal.
Q2	Having reviewed the tender documentation, we would appreciate clarification on the following points: - Could NTCSA provide an indication of the expected deployment scope, including the approximate number of substations, control centres, RTUs/gateways and OT assets anticipated to form part of the initial implementation? - Is the implementation expected to be deployed across all Transmission OT environments from project inception, or will deployment occur in phases? - Could NTCSA provide guidance on the expected security event volumes (EPS), log volumes and required retention periods for security events and forensic data? - Is monitoring expected at every substation and OT site, or will monitoring at selected aggregation, control centre or regional locations be considered acceptable? - Does NTCSA require passive OT asset discovery capabilities as part of the solution, or will integration with existing OT asset inventories be accepted? - Can NTCSA confirm whether event correlation, threat hunting and incident management capabilities are required to be provided natively within the proposed OT SIEM platform, or whether an integrated architecture consisting of an OT monitoring platform and a separate SIEM/SOC platform will be considered compliant? - Does the scope include the provision of 24x7 operational monitoring and SOC services, or is the requirement limited to the implementation, enablement and support of the technology platform? - Are there any specific utility, transmission or critical infrastructure reference requirements that will be evaluated beyond those already contained within the tender documentation? We appreciate your assistance and look forward to your response.
A2	This level of information will be made available to the successful supplier. Guidance in terms of sizing of the solution can be found in A1 (Daily Data Volume) and the BoQ. Since this is an enabling agreement (“as and when required”), the initial scope cannot be confirmed.

	Tender Questions and Answers	Document Identifier	240-7124948	Rev	1
		Effective Date	01 July 2024		
		Review Date	July 2027		

Number	Clarification / Discussion
	2. Since this is an enabling agreement (“as and when required”), the initial scope cannot be confirmed. 3. See A1. 4. Logs from all log generating devices across the network, irrespective of physical location. 5. Yes asset discovery capabilities for enabling the functionality of the solution should be offered as part of the solution. 6. The proposed/offered solution, without external dependencies should be able to fulfil this requirement. 7. This requirement is limited to the implementation, and enablement of the proposed solution. For support this requirement will be on an ad hoc basis (e.g., during a P1 – Emergency event, as defined in doc no.:240-135089195). 8. None. Any other technical evaluations will be with the successful supplier for the designs.
Q3	We are currently reviewing the tender: Design, Supply, Delivery, Installation, Commissioning, Maintenance, Support and Training of an Operational Technology (OT) Security Information and Event Management (SIEM) Solution for a Period of Five (5) Years – E2024NTCSAMWPR. Please see the attached clarification questions, which will assist us in putting together a quality and comprehensive proposal response aligned to Eskom’s requirements.
A3	Please see, answers A1 – A2 above, and refer to Appendix A, below for specific answers to the spreadsheet provided.
Q4	We refer to Tender E2024NTCSAMWPR and would appreciate your guidance on the following requirements, as they are important to our bid/no-bid assessment: Clause 3.2.3.12 ECSA-registered engineer sign-off: Kindly confirm whether this is a mandatory requirement and whether a bidder without access to an ECSA-registered engineer would be disqualified. ISO 14001 certification: Kindly confirm whether ISO 14001 certification is mandatory and whether a bidder that does not currently hold this certification would be ineligible to submit. ISO 45001:2018 certification: Kindly confirm whether ISO 45001:2018 certification is mandatory and whether a bidder that does not currently hold this certification would be ineligible to submit. For each item, we would be grateful if you could indicate whether it is: a mandatory eligibility requirement; a preferred or scored requirement; or

	Tender Questions and Answers	Document Identifier	240-7124948	Rev	1
		Effective Date	01 July 2024		
		Review Date	July 2027		

Number	Clarification / Discussion
	a requirement applicable only after contract award. Your clarification will be greatly appreciated and will assist us in making an informed decision regarding our participation in the tender. Thank you for your assistance.
A4	ECSA registration is not mandatory since NTCSA engineers will form part of the design team and also sign-off on the design documents.

	Tender Questions and Answers	Document Identifier	240-7124948	Rev	1
		Effective Date	01 July 2024		
		Review Date	July 2027		

Appendix A

QUESTION	RESPONSE
1 Can you provide high-level network architecture diagrams for all three OT systems?	This will be made available during the design with the prospective supplier who will sign the non-disclosure agreement.
2 Are there separate trust zones (e.g., Level 0-5 Purdue model) that must be respected?	Yes
3 What compute, storage, and virtualization standards exist (e.g., VMware, bare metal)?	The supplier should propose a suitable solution. The hardware should be part of the solution.
4 Are there approved hardware platforms/vendors?	No
5 Is there existing storage infrastructure (SAN/NAS) we must integrate with?	Yes
6 Are there any space, power, and rack constraints at deployment sites?	NTCSA will make the rack space and AC power available
7 Under what conditions is external connectivity allowed, if any?	No external connectivity allowed.
8 How should threat intelligence updates be handled in offline environments (manual upload processes)?	Manual update.
9 Are there existing threat intelligence subscriptions?	Yes
10 Are there preferred standards beyond STIX/TAXII?	As per specification the minimum is STIX/ TAXII. The supplier can propose any standard of their choice.
11 What specific OT/ICS technologies and vendors are in use (e.g., SCADA vendors, RTUs, PLCs)?	This will be made available during the design with the prospective supplier who will sign the non-disclosure agreement.
12 Which ICS protocols need to be monitored (e.g., IEC-104, DNP3, Modbus)?	at the minimum, MODBUS, MDLC, OPC, DNP3, GOOSE, IEC101/103/104
13 Are there any existing OT monitoring tools (e.g., network sensors, NDR)?	NTCSA has deployed the NIDS and NDR solution. The details will be communicated with prospective supplier during the design.
14 What IAM systems are in use (AD, LDAP, TACACS)?	LDAP
15 Is multi-factor authentication (MFA) required for SIEM access?	Yes but during the design we will need to unpack the use cases.
16 Is there an existing ticketing or ITSM system to integrate with?	The supplier should propose a ticketing/ ITSM solution as part of the support offering.
17 Are there privileged access management (PAM) tools integrated?	No.
18 What is the current incident response process/workflow?	Yes. The supplier must respond with their incident response plan.
Which regulatory frameworks must be supported:	
19 -NERC CIP?	Yes but not limited to those listed.
-Local South African regulations?	
-Internal Eskom standards?	
20 Are there specific audit reporting templates required?	The supplier to propose the reporting template based on their solution.
21 What is the expected log volume (EPS + GB/day)?	See answer A1 to Q1 on the clarification above.
22 What exact OT/ICS systems and protocols must be monitored?	at the minimum, MODBUS, MDLC, OPC, DNP3, GOOSE, IEC101/103/104
23 What is the network architecture (air-gap vs partial connectivity)?	Air-gap
24 Is there an existing SIEM or SOC capability?	No
25 What are the top 10 priority use cases (e.g., insider threat, OT anomaly detection)?	The capability to integrate up/northbound, should it be required for SOC purposes.
26 What integration with enterprise SIEM/SOAR is required?	The supplier should propose
27 What is the required availability architecture (active-active vs standby)?	Active-active for the two systems to be deployed.
28 What is the support model (self-managed vs managed service)?	Self managed
29 What is the expected data retention volume vs storage capacity available?	See answer A1 to Q1 on the clarification above.
30 Will Eskom fully operate the SIEM, or expect vendor-managed services?	NTCSA will be operating its SIEM solutions but there is a requirement for the prospective supplier to provide the service on an as when required basis
31 What level of skillset currently exists internally?	No skillset exist currently but the prospective supplier will be required to offer training to NTCSA personnel.
What are the expectations for:	
32 On-site support vs remote support?	On site support. Refer to the section 3.6.2 of Generic requirement for Telecoms contract.
-Response times beyond SLA tables?	
33 Are there requirements for local South African support presence?	Yes
34 What is the target audience for training (analysts, engineers, admins)?	Refer 3.8 of Generic requirement of the Telecoms contract
35 What level of certification or competency is expected post-training?	The supplier to propose.
36 What is the expected depth and duration of training programmes (basic vs advanced)?	Refer 3.8 of Generic requirement of the Telecoms contract
37 What is the expected transition timeline?	As soon as NTCSA have been trained.
38 Are there constraints on CAPEX vs OPEX?	This will be an enabling agreement (i.e., on an "as and when required basis")
39 Will Eskom provide access windows and schedules for deployment activities in OT environments?	Yes
40 Will Eskom provide on-site technical resources during deployment, or is the supplier expected to be fully self-sufficient?	NTCSA will provide on-site technical resources to assist with the deployment
41 Will Eskom require formal design presentations to technical committees?	Yes
42 What is the expected support delivery model (on-site, remote, hybrid)? Eskom mentions a dedicated resource so need to clarify on this item.	On site support. Refer to the section 3.6.2 of Generic requirement for Telecoms contract.
43 Is there a requirement for a dedicated service manager or account team?	Service manager is required.
44 Will Eskom require on-site support resources stationed permanently or periodically?	Periodically
45 What level of incident triage, investigation, and escalation is expected from the supplier?	Until our resources have been trained, it will cover the entire scope. Training is part of the scope and will ideally be initiated prior to the system being commissioned. After that only expert support/level 3 will be required from the supplier.
46 Should the supplier provide continuous threat hunting and proactive analysis?	Yes on an as and when required basis per SLA.
47 What incident management processes and tools are currently in place (e.g., ITSM platforms)?	The supplier should propose an incident management process and tools to be used as part of the support offering.
48 How should incident escalation and communication flows be structured between Eskom and supplier?	The supplier should propose as part of their ticketing offering.
49 Will the supplier be required to participate in incident response and recovery activities?	Yes
50 Is there a requirement to produce post-incident reports and root cause analyses?	Yes