PART A REQUEST FOR A REQUEST FOR INFORMATION (RFI)			
Description of the works/goods/services	Request for Information is required to identify Cloud and Edge Computing technologies deployment and cybersecurity implementation approaches, strategies, and architectures, applicable to NTCSA Operational Technology (OT) environment.		
Deadline for submission	22 July 2026	**At (South African Standard Time)**	10:00 AM
Tender Office address	Tenders are uploaded via NTCSA Tender bulletin site on the Eskom E-tendering page.		
RFI are to be submitted electronically via Eskom E-tendering site by the stipulated closing date and time. ***Please note it is the responsibility of the supplier to ensure that RFI submission is submitted before the closing date and time***	Suppliers are not allowed to submit physical files to NTCSA/Eskom Tender Offices. Please note it is the responsibility of the supplier to ensure that RFI submission is submitted before the closing date and time.		
Electronic Submission of RFI	The tenderer must upload the tender via NTCSA Tender bulletin site on the Eskom E- tendering page. All documents need to be submitted in a PDF and Excel format (The limit is 50MB per file and total submission of 900MB per submission). No Zip/condense files can be uploaded No hard copy will be accepted If for some reason you resubmit your EOI, then the latest version of the EOI submitted will only be accepted and all previous submission/s will be null and void. Please ensure that the submission status is indicated as complete. Supplier Help Manual guide and video can be found on Eskom E-Tendering page		

E-tendering Help Manual for supplier	Refer to the attached E-tendering Help Manual for suppliers

National Transmission Company South Africa SOC Ltd ("NTCSA") invites you to submit an:

- **Request for information (RFI)** is required to identify Cloud and Edge Computing technologies deployment and cybersecurity implementation approaches, strategies, and architectures, applicable to Eskom NTCSA Operational Technology (OT) environment.

NTCSA has delegated the responsibility for this RFI to the signatory of this document, whose details can be found below.

We look forward to receipt of your response.

Yours faithfully

Name	**Designation**	**Signature**	**Date**
Claire Gontse Sennelo	Asst Officer Procurement		01/07/2026
Telephone number	011 800 8111	**Fax and/or e-mail address**	Sennelcg@ntcsa.co.za

PART B **RESPONSE SHEET IN TERMS OF A REQUEST FOR A FOR INFORMATION** **To be completed by the supplier**			
To	NTCSA SOC Ltd	**Date**	
Attention			
Tel no		**Fax no and /or e-mail address**	
From		**Address**	
Address			
Sender			

Description of the works/goods/services	Request for Information is required to identify Cloud and Edge Computing technologies' deployment and cybersecurity implementation, approaches, strategies, and architectures, applicable to NTCSA Operational Technology (OT) environment.

Suppliers are to note the following:

- Responders are encouraged to refer to the stated requirements and expand on them where necessary, clearly indicating assumptions, deviations or value-added capabilities.

Please find below our response to NTCSA's questions:

No.	Question	Please indicate your response in this column
1.	Contact Information and Company Details • Your contact's name and contact details • Company registration number	
2.	Brief description of previous experience with ICT related or similar solutions for power utility OT solutions and applications.	
3.	What is the maturity of cloud and edge technologies within EPUs, for OT applications? Which applications are prevalent in using these technologies? *(Refer to maturity requirements)*	
4.	Which architecture do you support (e.g. cloud, edge, and/or cloud-edge) and why? Provide a typical high-level architecture design in an end-to-end power utility environment (i.e. from primary plant to control centre).	
5.	For cloud, which deployment architecture (i.e. Service and deployment models) do you support and why?	
6.	How do you define your cloud-edge (if applicable) architecture model for mission-critical utility environments and what criteria is used to determine workload placement (cloud vs edge vs on-prem, etc)? *(Refer to Technology Capability requirements)*	
7.	Does your architecture make allowance for grid control, and if so, how do you ensure low-latency performance for time-sensitive operations? *(Refer to Technology Capability requirements)*	
8.	How is data partitioned and processed across edge and cloud layers? What strategies are used for real-time analytics vs batch processing? *(Refer to Technology Capability requirements)*	

9.	What legacy OT systems and protocols (e.g., existing SCADA, EMS, DMS platforms and associated legacy communication protocols) can you integrate with, and how have these integrations performed under real incident or outage scenarios in live, brownfield utility environments? How do you ensure minimal disruption during integration with live systems? *(Refer to Integration requirements)*	
10.	How do you design for high availability and fault tolerance at both edge and cloud layers and what mechanisms are used to maintain this if cloud connectivity is lost? *(Refer to Performance and Scalability requirements)*	
11.	What are your SLAs for uptime, failover, and recovery and how do you test and validate disaster recovery scenarios? *(Refer to Performance and Scalability requirements)*	
12.	How are these SLAs contractually defined, tested, validated and audited over time (e.g. success criteria and evidence provided to customers)?	
13	What network architectures do you use for secure and resilient edge-to-cloud connectivity and how is intermittent or constrained connectivity in remote locations handled? *(Refer to Performance and Scalability requirements)*	
14.	What is your cybersecurity architecture for cloud-edge deployments in critical infrastructure? What security principles are enforced (e.g. Zero-trust, Purdue model etc.) *(Refer to Security and Compliance requirements)*	
15.	How does your solution scale across multiple substations or grid regions? What benchmarks or KPIs do you use to measure system performance and how are burst workloads or sudden spikes in demand handled? *(Refer to Performance and Scalability requirements)*	
16.	How do you ensure vendor interoperability in multi-vendor environments, and how is vendor lock-in avoided? Are your solutions based on open standards or proprietary frameworks, or both? *(Refer to Technology Capability requirements)*	
17.	What partnerships do you maintain with cloud providers and how is data migration handled from legacy systems to cloud platforms, as well as between	

	cloud platforms. How is business continuity ensured/guaranteed? *(Refer to Migration Consideration requirements)*	
18.	What tools do you deploy for end-to-end observability (edge to cloud) and how do you handle incident detection and response? What is your support model for 24/7 mission-critical environments? How do you perform root cause analysis in distributed systems? *(Refer to Operation and Support requirements)*	
19.	What pricing models do you offer (CAPEX vs OPEX, subscription-based)? What are the hidden or indirect costs if any (e.g. connectivity, data egress, maintenance)? *(Refer to Cost and Commercial requirements)*	
20.	What infrastructure is required to enable a cloud and edge ecosystem in an EPU OT environment (hardware, specifications, and data centre requirements)? Please provide a bill of materials (BOM) with associated indicative pricing.	
21.	What emerging technologies are you incorporating? What is your roadmap for supporting next-generation grid capabilities such as smart grids and Distributed Energy Resources (DER) integration? *(Refer to Use Case requirements)*	
22.	What skills are required for designing, implementing, operating and maintaining cloud and edge technologies? *(Refer to operation and support requirements)*	
23.	Please provide case studies of previous deployments that you have successfully completed for EPUs with reference to the following: a) Describe the reference architecture implemented? b) What role do standards such as IEC 61850, IEC 60870-5-101/104, DNP3, Modbus, etc play in your architecture? c) What were the key drivers for adopting cloud/edge in this deployment(s)? d) What data is processed locally vs centrally, and why? e) How do you manage data sovereignty and regulatory compliance in this deployment(s)?	

	f) What compliance frameworks do you adhere to (e.g. NIST, ISO standards)? g) How is identity, access control, and device authentication managed at scale? h) What hardware platforms are supported at the edge (ruggedized, substation-grade, etc.)? i) How do you manage remote lifecycle operations (provisioning, updates, patching)? j) What orchestration tools do you use (e.g., Kubernetes, containers, or edge-specific variants)? k) How are distributed edge nodes monitored and managed? l) What were the implementation timelines and what deployment approach was used (i.e. phased vs full deployment)? What are the top lessons learned from your utility deployments? What were the biggest challenges, and how were they mitigated?	
24.	Are you able to present and demonstrate the solutions to NTCSA in a live or simulated environment?	

Yours faithfully

Name	Designation	Signature	Date
[insert your full name/s]	***[Insert your full designation]***		
Telephone number		**Fax and/or e-mail address**	