KENYA ELECTRICITY GENERATING COMPANY PLC.

KGN-HYD-010-2019.

TENDER FOR SUPPLY OF SCADA HARDWARE FOR SEVEN FORKS & TURKWEL HYDRO ELECTRIC POWER PLANTS –KENYA.

15th May, 2019.

In Accordance with the "Tender for Supply of SCADA Hardware for Seven Forks & Turkwel Hydro Electric," KenGen hereby issues **Clarification No.2 & Addendum No.2.**

CLARIFICATION NO 2

Item No.	TENDER CLAUSE NO.	TENDER ARTICLE	Question/additional information sought by tenderers.	Clarification
8	SECTION I:	INVITATION TO TENDER.	On Joint Ventures – is site visit by one party enough for a JV?	Yes
9	5.2.3	SCADA RCC SERVER CABINETS SCOPE OF SUPPLY	On Cisco Ethernet switches - can bidders quote for from any other vendor so long they meet the technical requirements?	As per tender specifications, see tender clauses 5.2.3.5 and 5.4.2.8
10	5.2.10	SOFTWARE SCOPE OF SUPPLY	Some servers have Win Server 2012 and others have Win Server 2016. Can we standardize on 2016? The reason for this is that the two OS's require a 6th generation and 7th generation CPU respectively; hence, this influences the specification of the PC. - If 2016 is preferred, please confirm if the PLC or SCADA software is compatible with this version. -Also confirm which version is required for the Virtual Machines.	Windows server software to be provided and Licensed as detailed in tender clause 5.2.10, 5.4.1.3.3, 5.4.2.4 and 5.4.2.5.5,
11	5.4	PARTICULAR TECHNICAL SPECIFICATIONS	For Virtual Software to run more stable, Solid State Hard Drives are recommended. Should we replace all HDD's with SSD's	Please see tender clauses: 5.4.1.3.2, 5.4.2.2.2 and 5.4.2.5.2

Item No.	TENDER CLAUSE NO.	TENDER ARTICLE	Question/additional information sought by tenderers.	Clarification
12			Kindly confirm that VM Ware will handle the Virtual CPU creation and management On the Virtual Machine architecture and software	Please see tender clauses: 5.2.10.2.1, 5.2.10.5, 5.2.10.7.6, 5.4.1.3.3 and 5.4.2.3.1
13	5.4.5	CYBER SECURITY	Can bidders quote for Enterprise Cyber Security Appliance/Gateway from any vendor so long they meet the technical requirements?	(i) Cyber security solution and equipment to be supplied as per tender specifications. (ii) All Cyber security equipment and services **MUST** be from the same vendor
14			Should the desired ICS/SCADA Security devices must be a layer 2 device? Being on Layer 2 the security appliance can be placed anywhere on the L2 network and can secure the ICS/SCADA system without making Layer 3 network changes	The ICS/SCADA security devices must fully support the defined minimum requirements (security protections) for both Layer 3 and Layer 2 deployments. All security appliances MUST be layer 3
15	5.4.5.3	Technical Specifications cyber Security Functions	Should the proposed Solution be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports?	The solution should secure the traffic using all the minimum required security features/protections irrespective of the communication ports used or traffic encryption used. Refer to tender clause 5.4.5.3.2, 5.4.5.3.3
16			Should the proposed Solution be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed towards?	The solution must focus on automatic prevention of threats. Real-time dashboards must provide visibility of all identified threats. Refer to tender clause 5.4.5.3.7.
17	5.4.5.3.5	Sandboxing and File Scrubbing	What type of Sandboxing solution will be preferred (on-prem or cloud)?	(i) The proposed solution must fully support on premise sandboxing. (ii) The cyber security appliances shall support this service, but it shall not be enabled/activated if a separate license is required
18	5.4.5.3.3	Intrusion Prevention System	Should the detection engine incorporate multiple approaches for detecting threats including at a minimum, exploit-based	Section 5.4.5.3.3 defines the minimum IPS requirements.

Item No.	TENDER CLAUSE NO.	TENDER ARTICLE	Question/additional information sought by tenderers.	Clarification
			signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported?	
19			Should the IPS component also include URL/IP/DNS reputation scoring over and above base signatures, virtual patching (network layer), virus and malware detection?	The IPS minimum requirements are defined under clause 5.4.5.3.3, clause 5.4.5.3.4 specifies protections for viruses and bots, Clause 5.4.5.3.5 specifies protections for unknown malwares

ADDENDUM NO.2

Tender Submission Deadline

The tender has been extended from ~~21st May, 2019 at 10.00 a.m.~~ to 31st May, 2019 at 10.00 a.m.

ACKNOWLEDGEMENT OF CLARIFICATION NO. 2 & ADDENDUM NO.2

We, the undersigned hereby certify that the clarification is an integral part of the document and the alterations set out in this clarification have been incorporated in the tender proposal.

Signed……

Tenderer…….....

Date……