ADDENDUM I

10TH JUNE 2019

To All Tenderers

TENDER NO: KNEC/SEQIP/ONT/2018 - 019/03

TENDER FOR SUPPLY, INSTALLATION, TRAINING, COMMISIONING AND MAINTENANCE OF A SECURITY INFORMATION AND EVENT MONITORING SYSTEM AND NEXT GENERATION FIREWALL.

CLARIFICATIONS FOR QUESTIONS ASKED AND RESPONSES GIVEN BY KNEC

1. **Kindly clarify on number of years of support, one section mention 5 and another mentions 3.**

   KNEC Response: Support is for 1 year

2. **How many staff are to be trained on SIEM?**

   KNEC Response: Please refer to the scope of work (Page 101) which captures comprehensively issues to do with training. For technical staff Six (6) staff members

3. **Is high availability needed for the SIEM?**

   KNEC Response: No, Only one device required at our primary center

4. **Is there a preferred SIEM license or should we propose what we think is best per RFP?**

   KNEC Response: This is an open tender and bidders are to respond as per the specifications giving their solutions to the specifications given.

5. **How many sites will the SIEM be deployed to.**
   KNEC Response: The solution will be deployed at Primary data center. The SIEM should get the logs from all devices across all KNEC 4 sites since they are interconnected.

6. **We need the below information from the client environment. If more than 1 site indicate qty at each site.**

KNEC RESPONSE: Refer to Page 109 for issues raised below

Estimated Count of Event Log Sources	
AD/Auth, DHCP, DNS, ESX, O365	As per specifications page 109
Web and Mail Servers	As per specifications page 109
Windows General Purpose Servers	As per specifications page 109
Linux/Unix General Purpose Servers	As per specifications page 109
Antivirus, Anti-Malware Servers	As per specifications page 109
Database Servers	As per specifications page 109
Proxy Servers, Edge/Small Firewalls	As per specifications page 109
Core/Large Firewalls	As per specifications page 109
IDS, IPS, VPN, WAF, DAM, DLP, LB	As per specifications page 109
Routers, Switches, Wireless	As per specifications page 109
Other? (Indicate event rate)	As per specifications page 109
Other? (Indicate event rate)	As per specifications page 109
Other? (Indicate event rate)	As per specifications page 109

7. **Client to kindly indicate the below:**

Licensing Components	**Qty**
Estimated Events per Second (EPS)	Between 10000 to 15000 (minimum)
Estimated Flows (Sockets) per	Based on your proposal

8. **Other pertinent information:**

KNEC RESPONSE: Refer to Page 109 for issues raised below

Environment Information (Entire Environment):	
Total Number of Workstations (laptops/workstations) in the environment	As per specifications page 109
Total Number of Servers in the environment	As per specifications page 109
Throughput Needs for Q-Flow, QNI or QIF (Probes)	As per specifications page 109
Number of Major Data Centers/Collection Hubs	As per specifications page 109

Remote locations with local storage requirements	all data is local
Available WAN Bandwidth (For streaming logs)	20 MB mpls
Total number of Qradar Users Expected	As per specifications
System Preference (Virtual, Cloud, Appliance, etc.?)	AS per specifications refer pager 106 , in table point 2
Anticipated Growth Percentage	10%
Resiliency (HA and/or DR) Requirements	Not Applicable
On-Line Log/Flow Retention Req. (i.e. 1yr)	1 year