KENYA REVENUE AUTHORITY
ISO 9001:2015 CERTIFIED

Date : 16th March, 2020

KRA/HQS/NCB-063/2019-2020 – SUPPLY, DELIVERY, IMPLEMENTATION AND COMMISSIONING OF CYBER SECURITY OPERATIONS OF CYBER SECURITY OPERATIONS CENTRE SOLUTION

RE: ADDENDUM/CLARIFICATION SET "2"

Kenya Revenue Authority wishes to inform prospective bidders of the clarifications highlighted below for the tender no. KRA/HQS/NCB-063/2019-2020.

No.	TENDER DOCUMENT REFERENCE	CLARIFICATION QUESTION	CLARIFICATION RESPONSE
1.		Is there any SIEM solution already in place? If yes we need more details about the vendor and architecture, if yes do we need to replace it or to build on top of it the SOC?	**KRA already has IBM Qradar SIEM solution in place. The bidder expected to build on top of the SIEM, but not replace it.**
2.		What are the main services that KRA is looking to have in their SOC: o Log management? o Event management? o Advanced threat analysis? (expert rules and advance security analytics algorithms to reveal abnormal or suspicious behavior) oIncident triage?	**KRA seeks to automation Security operations and incident response activities, building on the already existing SIEM solution.** **Refer to section 4. Technical Requirements.**

16/03/2020

3.		Does KRA need to elaborate the process of the SOC activities? o(processes that covers alert monitoring, managing tickets, breakdowns and incidents, triage incidents, response to incidents, development and maintenance of the use cases and correlation rules and the collection, analysis and integration of information on threats)	**The proposed solution is aimed at achieving Security Automation and Orchestration (SOAR) to realize security operations automation and incident response capabilities, building on already existing SIEM solution in place. Refer to section 4. Technical Requirements.**
4		What are the KPIs required for the SOC activities	**To be determined at implementation.**
5.		Also we request an extension **of 20 days in** order to respond to your tender requirements exhaustively.	**The Tender has been extended to 24th March, 2020 at 11:00 am**
6.		Which existing SIEM do we need to integrate into in the new SOC	**Qradar SIEM.**
7.		Which solutions is KRA currently using for the following; 1. Firewall 2. Network Monitoring 3. End Point Protection 4. IT Ticketing System 5. Data Loss Prevention 6. Device Management 7. IDS/IPS 8. Patch Management 9. Incident Management 10. Vulnerability Assessment	**Key security solution platforms already provided. Details of specific security solutions in use to be provided after tender award.**

8.		How many SOC users does KRA want the New SOC to accommodate?	**Minimum of 5 users, scalable to 50 users.**
9.		Will the facility run 24/7?	**Yes.**
10.		What are the current SLAs for dealing with L1, L2, and L3 threats/incidents?	**Incident resolution SLAs:** **Critical - 2 hours** **High - 8 hours** **Medium - 24 hours**
11.		Is the SOC also expected to house and conduct data forensics capabilities? Currently, is this handled internally or externally at KRA?	**SOC forensics capabilities will be limited to endpoints.**
12.		Quantities for the Personal Computers is missing	**Ten (10)**
13.		Will KRA provide the server space for the software to be installed or the vendors to include that in their quotations	**Virtual environments will be provided for software based solutions. All solution software to be provided by the bidder. All other hardware required for the solution implementation to be provided by the bidder.**
14.		Does KRA have the design of the SOC or the bidders determine and present their designs? A site visit for the proposed SOC room is requested	**SOC design already there. The SOC monitoring site is under preparation and not ready for survey.**
15.		Why has "TAX Intelligence" been included in section (B) of page 27?	**Tax intelligence will be a critical component of the SOC. Tax intelligence sources to include but not limited:** ***a. Internal sources - KRA internal systems,*** ***b. External sources - deep web, Dark web, social media etc.***
16.		For the SOC, should we quote for spingback or fixed mounting of the wall screens?	**The bidder should propose the most ideal mounting option.**

16/03/2020

17.		In light of the above, we would like to request for at least 3 weeks of postponement of the the submission.	**The Tender has been extended to 24th March, 2020 at 11:00 am**

Note:

- Bidders are advised to acknowledge receipt of this addendum published and uploaded on the KRA Website on **16th March, 2020.**
- Prospective Bidders are hereby advised to align their Tender Security to the new tender opening date.
- This is the last and final set of clarifications in line with section II Clause 2.2.1 of the tender document.

Prospective bidders are advised that the notice of extension of the tender has been published via KRA E-Procurement Portal and KRA Website www.kra.go.ke
The Addendum form part of the bidding document and is binding to the bidder. All other terms and conditions of the tender remain the same.
This is the last and final set of clarifications in line with section II Clause 2.2.1 of the tender document.

You are therefore required to immediately acknowledge the receipt of this addendum through **eprocurement@kra.go.ke**

Regards,

Benson Kiruja
For: Deputy Commissioner - Supply Chain Management