KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

**Date : 10th March, 2020**

**CLARIFICATIONS TO TENDER NO.KRA/HQS/NCB-063/2019-2020**
**SUPPLY, DELIVERY, IMPLEMENTATION AND COMMISSIONING OF CYBER SECURITY OPERATIONS CENTER SOLUTION**

**RE: ADDENDUM/CLARIFICATION SET "1"**

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

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| 1 | 23 | ii). Vendor Evaluation | We like to highlight that number of SOC is a very secure subjects and customer are not willing to disclose names of the solutions used in SOC. Under NDA, Will KRA allow LPO or case study as valid document for cross reference for Deployment. Please confirm | **The bidders are required to submit reference letters supported by a copy of LSO or Completion certificate from the clients without mentioning the solution but an evidence indicating the service/ solution was implemented.** |
| 2 | 22 | SECTION V-SCHEDULE OF REQUIREMENTS | The Statement contradicts with Price schedule requirements. The Support duration is 3 years or 4 Years. Please confirm | **The support duration is 3 years.** |
| 3 | 26 | 3. Scope of Work | Please suggest if KRA is looking for bidder to propose OEM professional services from proposed vendor of the SOC platform. Engaging OEM during deployment and configuration will bring best practices, Guidelines, Recommendations from OEM (Original Equipment Manufacturer) for the supplied solution. | **KRA preference is to partner with OEM in implementing the proposed solution. The OEM will be required to guide and validate the design and architecture as well as provide quality assurance by validating and reviewing the implementation of the solution. The OEM is expected to provide technical assistance to** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | | **complement vendor capability for successful delivery.** |
| 4 | 27 | 3. Scope of Work | We understand that KRA is looking for Authorized OEM training from Authorized training partner of SOAR Platform.<br><br>Most of these trainings are usually conducted outside Kenya. We assume that KRA will bear the cost of travel, Visa, Accommodation for their employees. Please Confirm<br><br>We also believe KRA is looking for classroom based Instructor lead training and not online training. Please confirm | **Preference is for local training. However where not possible it can be delivered outside Kenya**<br><br>**In case of training outside Kenya, the bidder meets the training costs while KRA meets travel, visa and accommodation.**<br><br>**Classroom based Instructor lead training is required.** |
| 5 | 27 | 3. Scope of Work | To be able to derive on services required for the implementation of SOC solution, We will details and Qty of components that KRA is currently Using Defining following<br><br>a> Firewall - Make Mode & Qty<br>b> SIEM - - Make Mode & Qty<br>C> Antivirus - Make Mode & Qty<br>d> Antimalware - - Make Mode & Qty<br>e> Malware - Make Mode & Qty<br>f> PAM - - Make Mode & Qty | **a. Firewall – Checkpoint NGFWs**<br>**b. SIEM – QRADAR**<br>**c. Antivirus – Kaspersky**<br>**d. Antimalware – Kaspersky**<br>**e. Malware – Kaspersky**<br>**f. PAM - Cyber Ark** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | | |
| 6 | 28 | 4. Technical Requirements | Does KRA have existing threat intelligence feeds that will be integrated to the solution. If so, which are they? If not, should we propose threat intelligence feeds?<br><br>Kindly specify which sources of tax intelligence you would desire to integrate with and if there are any internal tax intelligence systems to be considered for integration. | **The bidder is expected to include proposed threat intelligence feeds integrated into the solution to ensure SOC is fully operational as described.**<br><br>**Tax intelligence sources to include but not limited:**<br>**a. *Internal sources - KRA internal systems,***<br>**b. *External sources - deep web, Dark web, social media etc.*** |
| 7 | 28 | 4. Technical Requirements | Please confirm if KRA is having any Helpdesk or Service Desk System with which the proposed solution is supposed to be integrated. Please Confirm if KRA currently has processes for Change Management, Incident Management, Problem Management etc. | **The solution is expected to support/have own incident management capability. KRA has Change Management, Incident Management, Problem Management processes.** |
| 8 | 28 | 4. Technical Requirements | How many endpoint clients should be factored in for the EDR solution.<br>Please also provide the operating system details for the various endpoints. Can we assume that endpoints are Windows systems. Please confirm | **Approximately 6,000 endpoints. About 95% running Windows systems and less than 5% running Mac and Linux systems.** |
| 9 | 28 | 4. Technical Requirements | EDR solution usually have antivirus and malware features. Can We assume that KRA is looking to replace their existing malware and antivirus solution. Please | **No, KRA is not seeking to replace the existing solution.** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | confirm | |
| 10 | 28 | 4. Technical Requirements | Does KRA have existing playbooks that should be automated or is the solution provider expected to build the playbooks. If the later, how many playbooks should we plan to build? | **KRA has no existing playbooks. Solution bidder expected to build approximately 20 playbooks. Exact number to be determined at implementation.** |
| 11 | 29 | 4. Technical Requirements | The functional requirement is very Open. To be able to define the costing for implementation effort, we will require exact details of both Internal and External systems with which integration is desired. | **The solution is expected to integrate with networking and communication infrastructure, servers, End points and various security solutions (mainly next generation firewalls, SIEM solution, anti-virus and anti-malware solutions, Active Directory, web application firewalls, privileged account management solutions) as well as well as external intelligence feeds including the deep and dark web.** |
| 12 | 29 | 4. Technical Requirements | We assume this requirement is for EDR. Please define the total count of endpoint agents from which EDR agent deployment is desired. | **Approximately 6,000 endpoints.** |
| 13 | 29 | 4. Technical Requirements | As informed in the prebid meeting that KRA is looking for HA for the SOC software, but the deployment of SOC will happen in Identified location within Times Tower. Please confirm<br><br>Additionally it was also informed during | **Server-side SOC hardware, software and data to be deployed/hosted in HA on the primary site with a DR arrangement on the secondary site** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | Pre-bid, that there is no DR SOC required. No software of hardware needs to be provided for Secondary SOC. KRA will backup the Data of the SOC solution at some other location. No Software needs to be provisioned for DR SOC. Please Confirm | |
| 14 | 29 | 4. Technical Requirements | We assume that Hardware, Operating System, Databases, SAN storage for the deployment of SOC system will be provided by KRA. We have to only provide hardware mentioned under Section 5. SOC Hardware Specifications. Please confirm | **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.** |
| 15 | 29 | 4. Technical Requirements | How many Security Analysts and Security Managers should the system be initially licensed for?. Can we assume that bidder has to provide SOC software with 5 Users . Please confirm | **Minimum of 5 users, scalable to 50 users.** |
| 16 | 30 | 5. SOC Hardware Specifications | We assume that SOC Software needs to be provided with 3 years Support and LED Display to be provided with 1 years Warranty. Please confirm | **Refer to Section 5. SOC Hardware Specifications** |
| 17 | 31 | 5. SOC Hardware Specifications | Please suggest the quantity of personal Computers to be provided | **Ten (10)** |
| 18 | 31 | 5. SOC Hardware Specifications | We assume that SOC Software needs to be provided with 3 years Support and Personal Computers to be provided with 1 years Warranty. Please confirm | **Refer to Section 5. SOC Hardware Specifications** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| 19 | 32 | 5. SOC Hardware Specifications | We assume that SOC Software needs to be provided with 3 years Support and Printers to be provided with 1 years Warranty. Please confirm | **Refer to Section 5. SOC Hardware Specifications** |
| 20 | 32 | 5. SOC Hardware Specifications | We assume that SOC Software needs to be provided with 3 years Support and LCD Projector to be provided with 1 years Warranty. Please confirm | **Refer to Section 5. SOC Hardware Specifications** |
| 21 | 33 | 5. SOC Hardware Specifications | We assume that SOC Software needs to be provided with 3 years Support and Shedder to be provided with 2 years Warranty. Please confirm | **Refer to Section 5. SOC Hardware Specifications** |
| 22 | 33 | 5. SOC Hardware Specifications | Please elaborate what accessories KRA is talking about. Can we assume that AC, Power, Racks, Virtual Environment ( for installation of SOC Software), LAN connectivity will be provided by KRA. We request KRA to allow Bidder to perform Site Survey to define the accessories they have to consider in their proposal. | **Network accessories e.g. patch cables/cords, cable ties/clips to support/connect Personal Computers, Printers, LED screens and shredder.**<br><br>**The SOC monitoring site is under preparation and not ready for survey.** |
| 23 | 34 | SECTION VII- PRICE SCHEDULE | Please confirm if KRA is looking for OEM Support or KRA is also looking for Bidder On Call support. Please confirm | **Manufacturer premier technical support services (including online support) required to complement bidder's on call support.** |
| | | | Which SIEM solution does KRA have? What is the EPS? How may log sources are already integrated with the SIEM | **SIEM Solution in use - QRADAR.**<br>**EPS – 5,000.**<br>**Approximately 500 log sources.** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | solution? | |
| | | | Is KRA expecting a big data based System which shall take care of SIEM + SOAR + Threat Hunting + EDR capabilities? | **Only SIEM solution already in place.** |
| | | | How many end points are to be considered for EDR? | **Approximately 6,000 endpoints.** |
| | | | For NTA – how many L3 switches are there? 1 GBPS or 10 GBPS? | **Clarification sought not clear** |
| | | | How many users are there in the organization? | **Approximately 8,000 users** |
| | | | How many quantity/units are required for the Personal Computer as per the below specification? | **Ten (10)** |
| | | | How many log sources you intend to integrate with the SIEM platform? | **Approximately 500 log sources.** |
| | | | Whats are the security technologies that Kenya Revenune use (Firewall, WAF, AV,...ETC) | **Firewall – Checkpoint NGFWs**<br>**WAF –F5**<br>**Antivirus – Kaspersky** |
| | | | We need more clarification for question "g" from Scope of work PG 27 is the training on the installed SOC Solution and how to manage the SOC? | **The training is on all solution components delivered. The bidder is required to build adequate capacity to enable the SOC team manage the solution competently.** |

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

| NO. | PAGE | TENDER DOCUMENT REFERENCE | CLARIFICATION QUESTION | CLARIFICATION RESPONSE |
|---|---|---|---|---|
| | | | Please specify how many Personal Computer are required since the Quantities are not provided for on PG31 under SOC Hardware | **Ten (10)** |
| | | | On Pg34 Under frame work contract please clarify on this | **The bidder is required to provide unit cost for one additional user above the minimum five required.** |

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 clarification/addendum form part of the bidding document and is binding to the bidder. All other terms and conditions of the tender remain the same.

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**