ADDENDUM 1

DATE: 22ND APRIL, 2026

TENDER NO. IEBC/OT/012/26/2025–2026

PROVISION OF SIEM & SECURITY MONITORING TOOLS

Pursuant to section 75(1) of the Public Procurement and Assets Disposal Act, 2015(Revised in 2022) the Commission hereby makes an addendum of the above tender as follows: -

| QUERY | RESPONSE |
|---|---|
| On page 75 and 76 there are a list of equipment but it does not really translate to Windows, Linux, MacOS, Unix and what needs to be patched. | • Patch Management will be implemented on the Commission's servers, which are 97 on Linux and 28 on Windows, and the 700 endpoints which are largely Windows based and approximately 30 on MacOS. Total estimated number of devices is 825. |
| How many servers and how many workstations. | • 125 servers (97 on Linux and 28 on Windows) and 700 workstations |
| NDR Requirement – Should a dedicated NDR solution fulfil this, or would SIEM-based NetFlow analysis capabilities be acceptable? If a dedicated NDR solution is required, can it be proposed as a virtual appliance (VM)? | • The provision of NDR and EDR solutions is not within the scope of this tender. However, the SOC platform shall provide an integrated dashboard capable of monitoring and interfacing with such solutions.<br>• A SIEM-based netflow analysis is acceptable for the SIEM solution. |
| EDR Requirement – Does the Commission require additional EDR agents beyond the current 100 deployed under the existing FortiEDR environment? If so, please confirm the required quantity. | • The Commission currently has an EDR solution and does not therefore require the provision of another EDR solution or additional agents. |

| | |
|---|---|
| On section c. Stage 3: Bidder evaluation (Technical Evaluation on capabilities matrix) the requirements for Project manager certifications specified are not aligned with PM role but are similar to technical experts' certifications. PM certifications aligned with the role are either Prince2 or PMP. Can this requirement be amended to align technical certification to technical experts and project manager certifications to project management role? | • The Project Manager is expected to have the certifications stated in the tender document, or equivalent. |
| SIEM is licensed on either Events per second and flows per minute or daily rates of data ingestion. The size of licenses to be provided is not indicated on the tender. How many EPS or FPM do you want procured? | • The ideal licensing should have 5000 Events Per Second (EPS) and 50,000 Flows Per Minute (FPM) |
| On SOC PLATFORM & ENDPOINT SECURITY section, the tender states requirement for NDR and EDR solution. Does IEBC want the solutions provided? and if yes please provide sizing to be used to license for both products | • The provision of NDR and EDR solutions is not within the scope of this tender. However, the SOC platform shall provide an integrated dashboard capable of monitoring and interfacing with such solutions. |
| The tender mentions sections on requirement for monitoring services. Does IEBC require bidders to provide Security Analyst to provide 24/7 monitoring services? If yes, how many analyst and will they be on site and remote monitoring services | • The bidder is expected to provide at least 2 security analysts, onsite, during the General Election period. |
| Specifically, we need clarification on the device count for patch management, whether the 700 BYOD devices are in scope for MDM, and the technical specifications for the 60k KIEMS devices. | • The number of devices for patch management are 125 servers (97 on Linux and 28 on Windows) and 700 workstations |
| Audited Financial Statements for the Year ended 31st December, 2025 are not ready. Could submit 2022, 2023 and 2024 | • Audited Financial Statements for the Year ended 31st December, 2025 has been waived.<br>• Bidder to submit Audited Financial Statements for the Year 2022, 2023 and 2024 |
| We request IEBC to allow JV partnership on both RFPs to aid provide the best suited proposal catering for all the solutions requested in the tender. | • The advertised tenders do not require JV partnerships to avoid unclear governance and accountability risks brought about by complexities of decision–making on technical approaches and project management. |
| What is the total number of log sources for the SIEM solution | • Approximately 870 |

| | |
|---|---|
| What is the number of Endpoints (Windows & Mac)? | • Approximately 825 |
| What is the total number of file servers | • 0 |
| What is the total number of domain controllers | • 2 |
| What is the total number of workstations required for vulnerability and patch management | • Approximately 825 |
| What is the total number of network devices required for vulnerability and patch management | • 45 |
| How many admins need access to the vulnerability and patch management application? | • Approximately 7 |

Clarifications/amendments form part of the bidding document and are applicable to all bidders. All other terms and Conditions of the Tender remain the same. Bidders who have already downloaded the bidding documents are required to acknowledge the receipt of these clarification/amendments. The tender closing date has been extended to **27th April, 2026** at 11:00 a.m. East African Time.

**Obadiah Keitany, MBS**
**For: Commission Secretary/CEO**