PRIVATIZATION COMMISSION

Enhancing Kenya's Productive Capacity

P.O. Box 34542 - 00100 Nairobi, Extelcoms House, 11th Floor Haile Selassie Avenue

Tel :+254(20)2212346/7/8 Fax :+254(20) 2212237 Email: info@pc.go.ke Website: www.pc.go.ke

**REF: TENDER NO. PC/10/2021-2022** **15/11/2021**

**TO: All Consultants participating in the RFP**

**RE: ADDENDUM NO. 1 – CLARIFICATION FOR RFP NO.: PC/10/2021-2022 – PROVISION OF VULNERABILITY ASSESSMENT AND BLACKBOX INTERNET PENETRATION TESTING FOR PRIVATIZATION COMMISSION**

Dear Consultant,

We have received some queries from some interested bidders on some issues relating to the above captioned RFP which we wish to clarify as follows:-

**Query 1: Tender Security amount is not indicated in the RFP document**

**Response:** The tender security for this RFP is Kshs. 100,000.00. The tender security shall be submitted with the technical proposal and shall be valid for a period of 120 days from the date of the tender opening. The tender security shall be denominated in Kenya Shillings or in another freely convertible currency and shall be in the form of:

a) A bank guarantee.
b) Cash.
c) Such insurance guarantee approved by the Authority.
d) Letter of credit

**Query 2: Bidder to provide evidence of having met International Data Centre Standards TIA - 942 or any other recognized international standard for tier 3 Data centre.** What's the equivalent of this requirement?

**Response:** Bidders are advised to use the terms of reference below which in essence respond to Query 2 above and effectively amend the terms of reference in the RFP document. This therefore means the terms of reference in the RFP document have been replaced by these ones below:-

## TERMS OF REFERENCE FOR PROVISION OF VULNERABILITY ASSESSMENT AND BLACKBOX INTERNET PENETRATION TESTING FOR PRIVATIZATION COMMISSION

### BACKGROUND

The Privatization Commission is a State Corporation established under Section 4 of the Privatization Act 2005). The Commission commenced its operations in January 2008, following the gazettment of Legal Notice No. 397 of 4th December 2008. Privatization Commission hereinafter referred to as PC, intends to procure Services for Vulnerability Assessment and Black Box Internet Penetration Testing at PC Headquarters.

Privatization Commission intends procure a firm to perform auditing, assessing information security risks and for compliance with the security policies, including vulnerability assessment and penetration testing of computer systems, networks and critical infrastructure. Rigorous penetration testing over Internet and Intranet should be carried out with intention to break the existing data security of PC. The weaknesses pointed out by such third party audits will enable PC to take effective and timely action to secure the ICT systems and networks.

### SCOPE OF AUDIT

The Scope of work covers evaluating the confidentiality, safety & security of the Data & Servers, assessing & strengthening the security posture of ICT systems and networks for protection against external threats, by way of remote infrastructure security assessment, Internal threats, by way of on-site infrastructure security assessment and Integrated system threats, by way of application security assessment on a quarterly basis.

The audit must address the following aspects:

1. Review current security policies & procedures and provide recommendations:

Review of organization ICT security policy and management system. Evaluating the current ICT Policy, Operational Procedure and Security Policy for processes that have been computerized:

i. Review of security procedures including Incident response

ii. Business continuity planning and disaster recovery

iii. Configuration management

iv. Recommending operational procedure and Security policy for these processes.

**2. Risk assessment and identification of security needs**

Evaluation of –

i. Current ICT infrastructure of Privatization Commission
ii. Network and the devices in use
iii. Operating systems
iv. Website
v. Database and Application packages
vi. Operational Procedures
vii. Identification of vulnerability, security flaws, gaps and loopholes
viii. Carry out Internal vulnerability assessment and External Penetration

**3. Review & Recommendation for Design of Security Architecture**

i. Evaluate the existing security architecture: recommend changes / new designs /layouts, and document the security architecture so as to conform to the International Standards and Industry-wide accepted best practices.
ii. The Security Architecture Design at the Head Office and the various interfaces used by applications on PC's network.
iii. Fixing the vulnerabilities in deployment of applications/systems, and recommend fixes for system vulnerabilities in design or otherwise for application systems and network infrastructure. Documenting the Security flaws, gaps and loopholes and fixing/addressing shortfalls which can be fixed immediately.

**4. Information Security Testing**

i. Posture Assessment
ii. Information Integrity Review
iii. Intelligence Survey
iv. Human Resources Review
v. Privacy Controls Review
vi. Information Controls Review

**5. Server/Workstation Penetration Assessment**

i. Server Hardening Review

ii. Workstation Hardening Review

**6. Process Security Testing**

i. Posture Review

ii. Request Testing

iii. Reverse Request Testing

iv. Guided Suggestion Testing

v. Trusted Persons Testing

**7. Internet Technology Security Testing**

i. Logistics and Controls

ii. Posture Review

iii. Intrusion Detection Review

iv. Network Surveying

v. System Services Identification

vi. Competitive Intelligence Scouting

vii. Privacy Review

viii. Internet Application Testing

ix. Exploit Research and Verification

x. Routing

xi. Trusted Systems Testing

xii. Access Control Testing

xiii. Password Cracking

xiv. Containment Measures Testing

xv. Survivability Review

xvi. Social Engineering

xvii. Distributed Denial of Service Testing

xviii. Security Policy Review

xix. Alert and Log Review

**8. Application Security Controls Testing**

i. Application Penetration Assessment

ii. Application Vulnerability Assessment

iii. Application Vulnerability Scanning

iv. Mobile Application Penetration Assessment

v. Remediation Support and Validation Testing

vi. Application Security Architecture Review

**9. Communications Security Testing**

i. Posture Review

ii. Modem Survey

iii. Remote Access Control Testing

iv. Voice over IP Testing

**10. Wireless Security Testing**

i. Posture Review

ii. Electromagnetic Radiation (EMR) Testing

iii. 802.11 Wireless Networks Testing

iv. Bluetooth Networks Testing

v. Wireless Input Device Testing

vi. Wireless Handheld Testing

vii. Wireless Surveillance Device Testing

viii. Privacy Review

ix. Physical Security Testing

x. Posture Review

xi. Access Controls Testing

xii. Perimeter Review

xiii. Monitoring Review

xiv. Alarm Response Review

xv. Location Review

xvi. Environment Review

## STATEMENT ABOUT WORK ON PRODUCTION SYSTEMS

The scope of work outlined above may be undertaken during normal working hours on production systems. The contractor MUST ensure no disruption of systems affecting the business of Privatization Commission is allowed to occur. It is also the contractor's responsibility to ensure that all data which may be accessed during the course of this work belonging to Privatization Commission, its clients or business partners is treated as strictly confidential.

## DELIVERABLES

1. A detailed project plan laying out the tasks to be undertaken and their associated timelines and tools to be used. This must be done two weeks before the audit
2. Provide a detailed quarterly report of findings identifying Application, Network, and Organizational vulnerabilities and the recommended remediation clearly indicating what was tested, how it was tested, and the results of the test. For prioritization purposes during remediation, the test findings should be ranked in order of importance for each detected vulnerability.
3. The final report must be available within three weeks of completion.
4. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing are reported immediately to Privatization Commission with a practical solution as soon as they are found.

## EVALUATION CRITERIA

| Requirements | | | Compliance |
|---|---|---|---|
| | Mandatory Requirements | | |
| | ▪ Must provide one original and one copy of the Tender which MUST be Paginated/serialized/Numbered on | | |

| | | | |
|---|---|---|---|
| | each page including all the attachments. The copies must be clearly marked 'Original' and 'Copy'. | | |
| | ▪ Copy of a Certified Company certificate of registration/ incorporation | | |
| | ▪ Accreditation by the ICT Authority of Kenya | | |
| | ▪ Copy of a Certified valid Tax Compliance certificate | | |
| | ▪ Copy of a Certified Valid Single Business Permit / County Business Permit | | |
| | ▪ Duly signed and stamped Anti-corruption declaration & statement on the bidder's letter head indicating that the person or his or her sub-contractor, if any, is not debarred from participating in procurement proceedings. | | |
| | ▪ Duly filled and signed Form of Tender | | |
| | ▪ Valid Tender Security of Kshs. 100,000.00 in the prescribed format. | | |
| | ▪ Bidders shall sequentially serialize all pages of each tender document submitted | | |
| | ▪ Bid MUST be submitted in the format required by the procuring entity - all the tender documents to be TAPE/BOOK and BOUND.<br>(Spiral Binding and use of Spring or box files will not be accepted and will lead to automatic disqualification) | | |
| | **Technical requirements Compliance** | | |
| | Relevant valid ISO Certification e.g. 27001 | 5 | |

| | | | |
|---|---|---|---|
| | Company Profile showing relevant experience in Cyber Security, ICT Audits, ISMS and related assignments.<br>• Relevant experience in ICT Audits, VAPT Services -15<br>• Project management of similar or related assignments - 10 | 25 | |
| | At least Three (3) completed Public Sector Related projects undertaken (provide references letters/ completion certificates and value of projects e.g LSOs and Contracts) | 15 | |
| | Provide project work plan | 10 | |
| | Staff Competency (Lead consultant-10 , Project Manager-5 & Technician-5)<br>Submit copies of signed staff CVs, fully supported academic & professional qualifications proving:<br>• Years of service with firm<br>• Education<br>• Experience<br>• Relevant certifications e.g. Cyber Security, ICT Audits, ISMS (provide evidence) | 20 | |
| | Detailed proposal on layout, methodology and set-up of the service | 20 | |
| | Documentation and proposed Service Level Agreement.<br>• Support contacts<br>• Turnaround times<br>• Escalation matrix | 5 | |

**Note: Bidder MUST score minimum of 80% to proceed to financial evaluation.**

**Query 3: Would the Commission consider a 1 week extension for the deadline of submission.**

**Response:** In view of the urgency with which the exercise needs to be undertaken, the Commission will not be in a position to extend the RFP submission deadline.

**Query 4: What is the number of systems that would be involved in the vulnerability assessment and penetration test for cost estimation purposes.**

**Response:** The Commission has the following systems and firmware setup:-

1. Dynamics Central ERP
2. Electronic Document Management System
3. Access Control system
4. CCTV
5. Storage Area Network (NetApp)
6. Wireless Access Points
7. Colocation site
8. Website Host (External)
9. E-Board
10. Segregated Network

**All the other terms and conditions of the RFP remain unchanged.**

**Sylvester Kamau**
**Manager Supply Chain Management**
**For: EXECUTIVE DIRECTOR/CEO**