Public Procurement and Disposal of Assets Authority

INTERNATIONAL COMPETITIVE BIDDING(ICB)

REQUEST FOR EXPRESSION OF INTEREST
(CONSULTING SERVICES – FIRM SELECTION)

ASSIGNMENT TITLE	**:**	**PROVISION OF CONSULTANCY SERVICES TO CONDUCT INFORMATION SECURITY AUDIT OF E-GOVERNMENT PROCUREMENT AND E-GOVRNMENT MARKETPLACE SYSTEMS.**
REFERENCE NUMBER	**:**	**PPDA/e-GP/12/2024**

1. Background

The Government of the Republic of Malawi (GoM) acknowledges the vital role that Information and Communication Technology (ICT) plays in promoting socio-economic development and empowering marginalized populations. One of the principles of public procurement contained in section 30 of the Public Procurement and Disposal of Public Assets is utilization of ICT. In line with this commitment, the GoM intends to implement an ICT initiative, specifically the Malawi National Electronic Procurement System(MANePS) – Phase II, under the Program for Results (PforR). The Public Procurement and Disposal of Assets Authority (PPDA) will serve as the implementation agency for this project.

The implementation of this initiative is designed to further the Government's overarching objectives in economic governance by systematically enhancing the efficiency and effectiveness of public procurement processes. This improvement will be applied across a diverse set of Procuring and Disposing Entities (PDEs), ultimately promoting transparency, reducing costs and ensuring that resources are procured optimally to achieve better outcomes for all stakeholders involved.

2. Objective of the Consultancy

The objective of the assignment is to undertake a comprehensive system security audit of the existing digital and physical infrastructures with the associated controls in place to effectively mitigate risks that could prevent the e-GP and e-GM systems from

accomplishing their business goals. Specifically, the audit agency is required to conduct:

a. Security Audit
b. Guide the client in getting the MANePS software documented
c. Evaluate Server Infrastructure Deployment & Data security
d. Verify the functioning of the service level measurement tools implemented in the e-GP / e-GM
e. Load testing of the e-GP / e-GM software
f. Penetration testing
g. Prepare the business continuity plan

3. **Scope of services:**

Specifically, the audit agency is required to conduct:

i) **Security Audit:** Evaluate security controls implemented in the application software vis-à-vis international best practices and make a recommendation on the remedial measures to be taken to comply with the prescribed global standards. Besides the application audit, the security audit shall review security controls in the database, operating systems, and network infrastructure setup.

ii) **Documentation:** Prescribe documentation requirements in a typical IT software implementation project (i.e., both software development and maintenance phases covering not only the software application but also the installation, implementation, and exit/transition management activities) and actively guide the team in getting the documentation done in line with the international standards.

iii) **Server Infrastructure Deployment & Data Security:** Evaluate the deployment architecture (server infrastructure) and actively guide the implementation team in the reconfiguration of the servers and storage such that load handling is distributed across the Servers and Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are kept as per industry standard. Especially, the server configuration and data security must be evaluated first-hand, and hands-on guidance should be provided to the implementation team in the reconfiguration of the server infrastructure where applicable. A robust data backup policy must be effectively implemented.

iv) **Service Level Measurement**: The e-GP vendor and e-GM vendors are required to comply with certain specified Service Level Requirements (SLR) such as page loading time and system availability. The audit agency is required to verify whether the service level measurement reports auto-generated using the tools deployed by the respective vendors accurately reflect the actual functioning of the e-GP system.

v) **Load Testing:** The e-GP and e-GM software must comply with certain load handling requirements. The audit agency must load the e-GP and e-GM systems onto a load testing tool to verify whether the software can manage the envisaged workload.

vi) **Penetration Testing:** Perform external penetration testing to identify vulnerabilities that could be exploited by users located outside the network

perimeter and provide hands-on guidance to the implementation team in strengthening perimeter security.

vii) **Business Continuity Plan**: Two aspects of business continuity have to be looked at: system administration and software development. Firstly, under system administration, the consultant needs to advise the client on the procedures to be established and identify the knowledge transfer which needs to take place to effectively ensure administration of the e-GP and e-GM systems using national resources. Besides playing an advisory role, the consultant needs to verify and confirm that the government is capable of deploying the source code and manage the servers. Secondly, the consultant is required to advise the government on the institutional set-up it needs to establish to effectively manage the source code and as required make changes to it using in-country expertise.

The eGM and eGP systems are designed to operate as distinct software applications. However, a single vendor is developing them, and from a functional perspective, the eGM has been integrated as a module within the eGP system. Both systems share essential supporting modules and system functions, including System Administration, Annual Procurement Planning, Identity Access Management, and Contract Management. Consequently, this integration allows the security audit agency to conduct comprehensive assessments of the two systems collectively.

Immediately after the contract signing, PPDA will ensure that a Task Order is issued to the audit agency to address the following assignment objectives:

a) Security audit
b) Documentation
c) Server Infrastructure Deployment & Data Security
d) Service Level Measurement
e) Business continuity plan

The estimated level of effort is 10 man-months over a period of two (2) years for the assessment of both e-GP and e-GM systems.

4. Qualification and Experience of the Consultant:

i) The bidder should be a registered firm functioning for at least 3 years as of the due date for submission
ii) The bidder must have successfully completed at least 3 IT Security Audit assignments within 3 years of the due date for submission
iii) The bidder must have at least 10 employees as staff on its payroll
iv) The bidder must have an average annual turnover of USD 0.5 Million from IT audit or IT consulting in the last 3 years.

5. Invitation for Expression of Interest:

The PPDA now invites eligible consultant firms to indicate their interest in providing the Services. Interested Consultant firms should provide information (including staff Resumes) demonstrating that they have the required qualifications and relevant

experience to perform the Services. The Consultant firm will be selected according to the procedures set out in applicable public procurement regulations in Malawi.

6. Submission of Expression of Interest:

Written expressions of interest (with CVs) marked "Selection of an Agency to Conduct Information Security Audit of e-Government Procurement and e-Government Marketplace Systems" must be delivered through electronic mail or in person to the address below on or before **14:00 pm local time on 10-January-2025.** The address referred to above is:

The Chairman
Internal Procurement and Disposal Committee
Public Procurement and Disposal of Assets Authority
Private Bag 383
Lilongwe
MALAWI
Tel: 265 887 083 265/3/4
E-mail: info@ppda.mw