DSLR/1421/2022-B7

Department of Survey and Land Records
'Survey Bhavan', Vazhuthacaud,
Thiruvananthapuram-695014
Ph: 0471-2325266, Fax: 2338210
E-mail: dydir1-tvm.syr@kerala.gov.in
19/12/2022

Tender Notice

The Department of Survey and Land Records, Government of Kerala invites financial bids from **CERT-IN EMPANELLED INFORMATION SECURITY AUDITING ORGANISATIONS** for conducting Application Security Audits for the Software Applications owned by the Department. The last date of submission of bids in protected pdf files as email on or before 27/12/2022 at 15.00 Hrs.

Sd/-

Director

Enclosure: RFP Reference No: **DSLR/1421/2022-B7 dated 19/12/2022**

by order.

സുരേശൻ കാണിച്ചേരിയാൻ
അഡീഷണൽ ഡയറക്ടർ
സർവ്വെയും ഭൂരേഖയും വകുപ്പ്
ഡയറക്ടറുടെ കാര്യാലയം
തിരുവനന്തപുരം-14

NOTICE INVITING FINANCIAL BIDS

FOR

ENGAGING SERVICE PROVIDER FOR SECURITY AUDIT OF THE SOFTWARE APPLICATIONS OWNED BY DEPARTMENT OF SURVEY AND LAND RECORDS, GOVT. OF KERALA

DSLR/1421/2022-B7 dated 19/12/2022

IMPORTANT INFORMATION

1	Inviting Officer	The Director, Department of Survey and Land Records
2	Last date & time for submission of bid	27/12/2022 at 15.00 Hrs
3	Bid Submission Mode	email as password protected pdf file
4	The Bid Document, complete in all respects, to reach at the address , on or before the due date	spmu.dslr@kerala.gov.in
5	Pre-Bid Meeting (Google Meet)	21/12/2022 at 15.00 Hrs Meet ID : meet.google.com/vep-xghj-zjo
6	Password Info sharing window (for the password protected pdf file)	After the last bid submission date and till 1 hr prior to bid opening time.
7	Date & time of opening of Bids	28/12/2022 at 11.00 Hrs

8	Venue for opening Bids	Directorate of Survey & Land Records, Survey Bhavan, Vazhuthacadu, Thiruvananthapuram -14
9	Contact Person for Queries	1. Pushpa.P.R mail id: spmu.dslr@kerala.gov.in procurementdslr1@gmail.com 2. Ravi J S mail id: spmu.dslr@kerala.gov.in procurementdslr1@gmail.com
10	Period of Completion of Work from the date of award of work	The vendor shall provide the first audit report not later than 2 weeks from the date of receiving the work order.

1. INVITATION OF BID

The Director of Department of Survey and Land Records (hereinafter referred to as DSLR) ,Government of Kerala (hereinafter referred to as the Department) invites financial bids from **CERT-IN EMPANELLED INFORMATION SECURITY AUDITING ORGANISATIONS** (hereinafter referred to as "Bidder" till the award of Contract and thereafter on award of contract, referred to as "Vendor/Contractor/Supplier/Successful Bidder") for conducting Application Security Audits for the Software Applications owned by the Department. The successful Bidder shall be finalized based on the competitive bidding process. Submission of bids shall be deemed to have been done after careful reading and examination of the document with full understanding of its implications.

2. PURPOSE , OBJECTIVE AND CONTENT OF THE ASSIGNMENT

The overall purpose of the Security Audit exercise is to confirm to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis with respect to CERT-IN guidelines. Application Security Audit covers some or all but not limited to the following activities

a) Identify the application level vulnerabilities on applications hosted in a test site/ production site based on the latest OWASP Top 10 vulnerabilities

b) On demand application scans

c) Password strength on authentication pages

d) Scan Java Script for security vulnerabilities

e) File inclusion attacks

f) Malicious File Uploads

g) Provide recommendations for remediation of identified vulnerabilities. The report should contain discovered vulnerabilities and description of vulnerabilities and mitigation or remediation recommendations for fixing and patching existing and found vulnerabilities as a part of solution.

h) Follow a specific format for reports.

i) Certify the applications/websites tested as "Safe for Hosting" and in times if Electronic Payment Gateway Operators request to provide it in their format.

j) Accept responsibility for declaring the websites/ URLs/ mobile applications free from known vulnerabilities

k) Any other activity concerning security audit related aspects, not essentially covered by work-areas outlined above.

3. SCOPE OF THE WORK

3.1 The selected vendor may cover the below mentioned tests for the application or website or Mobile App provided for testing.

1. Application Security Audit
2. Penetration Testing
3. Vulnerability Testing
4. Database Server Controls
5. Physical Access Control
6. Network security Review as part of Application Security
7. Compliance Review

3.2 Black box testing for Security Audit should follow OWASP guidelines covering the testing below.

1. Cross-Site Scripting (XSS)
2. Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
3. Input Validation flaws
4. Malicious file execution
5. Insecure direct object references
6. Cross-site request forgery (CSRF)
7. Information leakage and improper error handling
8. Broken authentication and session management
9. Insecure cryptographic storage
10. Insecure communications

11.Failure to restrict URL access

12.Denial of Service

4. OBJECT FOR THE SECURITY AUDIT

The Application/Website/Mobile App given in **Appendix 1A & 1B** are to be audited under this invitation.

5. DELIVERABLES

1. Report on All Items Found During Security Audit.
2. Threat assessment Reports detailing
    i. System flaws and weaknesses with remedial actions
    ii. Information leaks and exposures caused by such leaks with remedial actions.
3. Final Audit Certificate

6. INSTRUCTION TO BIDDERS

a. Only CERT-IN empanelled agencies will be eligible to submit the bids
b. The duly signed bids should be submitted via e-mail to address spmu.dslr@kerala.gov.in
c. Submission of bids will be as per the time schedule stated in this document.
d. In consideration of the bidder being allowed to quote for the work, bidder should keep the tender firm for a period of 90 days from the date of opening the bid during which period or till the bids are decided whichever is earlier, bidder will not be permitted to withdraw the bids
e. Late bids will not be accepted.

f. All pages in the document that forms part of the bid should be signed by the authorized signatory

g. Bid should accompany a Covering letter duly signed by the authorised signatory of the bidder.

h. The agency shall bear all costs associated with the preparation and submission of the Bid.

i. The Bid prepared by the Bidder, Supporting documents and printed literature furnished by the bidders as well as all correspondence and documents relating to the Bid exchanged between the Bidder and DSLR shall be in English.

j. The prices shall be quoted in Indian Rupees (INR) only.

k. The bidder is allowed to modify or withdraw its submitted bid any time prior to the last date prescribed for receipt of bids.

l. Subsequent to the last date for receipt of bids, no modification of bids shall be allowed.

m. If any agency submitted more than one bid, the one submitted recently to the last date and time of submission of bids shall only be considered.

n. The bidders cannot withdraw the bid in the interval between the last date for receipt of bids and the expiry of the bid validity period specified in the bid.

7. GENERAL TERMS AND CONDITIONS

i. The Director reserves the right to amend or cancel the bid invitation in part or in full without prior notice at any point of time.

ii. The bid inviting authority or other sanctioning authority reserves the right to reject any bid or all the bids without asking any reason thereof.

iii. If the Director deems it appropriate to revise any part of this invitation or to issue additional clarifications for interpretation of provisions of this document, bidder may issue supplements to this bid invitation. Any such

supplement shall be deemed to be incorporated by this reference to this document

iv. The successful bidder shall provide the first audit report to the department not later than 2 weeks from the date of receiving the work order. Subsequent interim reports shall be issued not later than 8 working days of receiving the patched application for re-test.

v. For any audit engagement, besides the original first audit, the vendor shall do any number of re-tests at no additional cost till all issues are cleared by the department within 90 working days of providing the first audit report. It should also ensure no new vulnerabilities are introduced as part of code changes to fix the reported vulnerabilities.

vi. The vendor may be terminated from audit engagements for reasons such as dishonouring audit commitments or violating these terms and conditions, degradation of auditor's performance or competence to meet expectations or if empanelment at CERT-IN ceases.

vii. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.

viii. For any audit engagement, the vendor shall provide support to the auditee technical team in fixing the security issues reported in first audit or any subsequent audit in terms of handholding and training. The support should include a minimum of 1 day onsite or remote training or handholding on how to fix the issues.

ix. The vendor shall adhere to all terms and conditions as per agreement with

CERT-India.

x. The vendor shall not subcontract any part of work assigned to another vendor or engage non-employees to perform the work.

xi. A formal Confidentiality & Non-Disclosure Agreement should be signed by the vendor to keep confidential all the information that it has access to during the course of its actions. Employees at the vendor organization should sign individual NDAS. As per CERT-In advisory, the empanelled vendor must ensure that data collected during audit work and reports prepared are not taken out of the auditee organization's premises/ network and/ or shared to anyone except the auditors, auditee organization, CERT-In and any other authorized Government entity. Any audit data should be wiped out from the vendor's domain after any engagement.

xii. In the case of Application Vulnerability Assessment/ Penetration Testing (VAPT), the Auditor will be required to audit and test the website on the staging server/testing environment provided by the hosting service provider before issuing the audit certificate.

xiii. The vendor may submit detailed proposals including,

1. Details of different tests/audits to be performed, standards against which the audits will be performed etc.

2. Details to include specific systems/subsystems to be audited and what activities will be performed in the subsystems

xiv. The whole process of starting the audit by the vendor till issue of final

audit certificate should be completed within 2 months

xv. The audit should strictly adhere to the guidelines specified for the purpose by Government of Kerala vide G.O (MS) No.8/2019/ITD Dated, Thiruvananthapuram,22.04.2019

8. FINANCIAL TERMS AND CONDITIONS

A. The rates should be quoted against each application/website/mobile app under this invitation, inclusive of all applicable taxes.

B. Rate shall be quoted on a per parameter basis, The parameters for quoting the rates are the number of

1. static pages
2. dynamic pages
3. input forms
4. input fields
5. user roles

C. For Audit of each application, the empanelled agency will share the TEST URL of each application proposed to be audited. After studying the application the agency will be required to submit proposals

9.SUBMISSION OF BIDS

1. Bids are to be submitted only in the format provided in **Appendix 2** to this document. Bids submitted in any other format shall be rejected.
2. The bids are to be submitted electronically in a password protected PDF document to ensure that they cannot be opened prior to the bid opening time.
3. The Financial bid, completed in all aspects and duly signed, shall

be sent the e-mail id spmu.dslr@kerala.gov.in so as to reach on or before the last date and time specified for bid submission.

4. The time of receipt of the bid document in the inbox of spmu.dslr@kerala.gov.in shall only be considered as the time of submission of bid. Department is not responsible for any delay or technical error whatsoever in the non-receipt or delay in delivering the bid to the above mail id.
5. Bidders are required to share the password to open bid document to spmu.dslr@kerala.gov.in after the last date prescribed for the submission of bids till 1 hr prior to the bid opening time.

10. AWARD OF WORK ORDER

1. The L1 bidder will be awarded the contract provided the purchase committee is sufficiently convinced after the evaluation of bids.
2. The acceptance of the bid will be intimated to the successful bidder by the Director through e-mail prior to expiry of the period of the bid validity.

11. PAYMENT TERMS:

I. No mobilization advance shall be paid.

II. 50% payment of the charges may be paid to the vendor on submission of the first Audit report. Balance 50 % will be released only after issue of the final audit report and Security Audit Certificate.

III. The payment shall be released to the vendor on submission of Bills (invoices) in Triplicate addressed to The Director, Department of Survey and Land Records, Thiruvananthapuram.

12. RIGHT TO TERMINATE PROCESS

i. The Director may terminate the bidding process at any time without assigning any reason. The Director makes no commitments, expressed or implied that this process will result in a business transaction with anyone.

ii. This bid Document does not constitute an offer by the Department. The bidder's participation in this process may result in the Department selecting the bidder to engage in further discussions and negotiations toward execution of a contract. The commencement of such negotiations does not however signify a commitment by the Department to execute a contract or to continue negotiations. Department may terminate negotiations at any time without assigning any reason thereof.

13. FORCE MAJEURE

For the purpose of this Article, Force "Majeure" means any cause, which is beyond the control of the vendor or the Department as the case may be, which such party could not foresee or with a reasonable amount of diligence could not have foreseen, and which substantially affect the performance of the Contract, such as:-

1. War / Hostilities
2. Riot or civil commotion
3. EarthQuake, Flood, Fire, Tempest, Epidemics, Lightning or other natural physical Disaster, Quarantine restrictions and Freight embargoes
4. Restrictions imposed by the Government or other statutory bodies, which are beyond the control of the vendor, which prevent or delay the execution of the order by the vendor.

ii. In case of occurrence of the above mentioned cases, the successful bidder's right to an extension of the time limit for completion of the work in above-mentioned cases is subject to the following

procedures.

1. That within 10 days after the occurrence of a case of Force Majeure but before the expiry of the stipulated date of completion, the bidder must inform the Department in writing about the occurrence of Force Majeure Condition and that the vendor considers himself entitled to an extension of the time limit.
2. That the vendor provides evidence of the date of occurrence and the duration of the force majeure in an adequate manner by means of documents drawn up by responsible authorities.
3. That the vendor proves that the said conditions have actually interfered with the carrying out of the contract.
4. That the vendor proves that the delay occurred is not due to his own action or lack of action.
5. Apart from the extension of the time limit, force majeure does not entitle the successful bidder to any relaxation or to any compensation of damage or loss suffered

14. CONFIDENTIALITY

Any information pertaining to the Department or any other agency involved in the project, matters concerning Government of Kerala and Government of India that comes to the knowledge of the vendor in connection with this contract, will be deemed to be confidential and the vendor will be fully responsible, for the same being kept confidential and held in trust, as also for all consequences of its concerned personnel failing to observe the same. The vendor shall ensure due secrecy of information and data not intended for public distribution.

15. LIMITATIONS OF LIABILITY

The liability of the Department for its obligations under the Contract shall in no case exceed the total value of the Contract.

sd/-
Director.

by order

സുരേശൻ കാണിച്ചേരിയാൻ
അഡീഷണൽ ഡയറക്ടർ
സർവ്വേയും ഭൂരേഖയും വകുപ്പ്
ഡയറക്ടറുടെ കാര്യാലയം
തിരുവനന്തപുരം-14

APPENDIX 1(A)

APPLICATIONS/WEBSITE/MOBILE APP OWNED BY DEPARTMENT OF SURVEY AND LAND RECORDS PROPOSED FOR SECURITY AUDIT

#	Application/Website /Mobile App	URL	Parameter and Range (in Nos)						Developer
			Static Pages	Dynamic Pages	Input Forms	Input Data Fields	User Roles	Screens (for mobile App)	
1	Entebhoomi portal	staging.entebhoomi.kerala.gov.in	0	900	500	1200	23	NA	NIC

APPENDIX 1(B)

APPLICATIONS/WEBSITE/MOBILE APP OWNED BY DEPARTMENT OF SURVEY AND LAND RECORDS PROPOSED FOR SECURITY AUDIT

Sl.No.	Web Application Assessment Details	Description
1	Web Application Name &URL	M.App Enterprises/staging.entebhoomigis.kerala.gov.in
2	Type of application Web/Application/ Mob/Rest / Thick / Thin instance to assesses & number of Application (s)	Cloud based application
3	How many login systems to assess?	7
4	How many static pages to assess? (Approximate)	7
5	Back-end Database	PostgreSQL
6	Authorization No. of roles & types of privileges for the different roles	Currently 2
7	Front-end Tool [Server side Scripts]	Java , .Net , C++
8	Operating System Details	Windows 2019 Std
9	Application Server with Version	IIS 10
10	Number of URL's require to assess?	7
11	Is it Thick or Thin Client Application	Thin
12	Is this Applications is ERP/ Enterprise based App	Enterprise based App
13	Is the Application previously audited or not?	Yes, Vendor Audited application

APPENDIX 2

FINANCIAL BID SUBMISSION FORM

FINANCIAL BID SUBMITTED TO THE COMMISSIONER OF LAND REVENUE FOR THE SECURITY AUDIT OF THE FOLLOWING APPLICATIONS/WEBSITE/MOBILE APP

Bid Submitted by : <organisation name>

Date of Submission : <Date>

#	Application/Website /Mobile App	URL	Parameters and Range (in Nos)						Cost inclusive of all applicable taxes (in Rs)
			Static Pages	Dynamic Pages	Input Forms	Input Data Fields	User Roles	Screens (for mobile App)	
1	Entebhoomi Portal	staging.entebhoomi.kerala.gov.in							
2	M.App	staging.entebhoomigis.kerala.gov.in							
Total									

Total Cost in Figures:

Total Cost in Words:

Authorised Signatory