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
12.01.2023

Quotation 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 file as email on or before 23/01/2023 at 15.00 Hrs.

Director

Sd/-

Enclosure: RFP Reference No: **No DSLR/1421/2022-B7 dated12/01/2023**

by order

P. R. PUSHPA
Deputy Director
Directorate of Survey & Land Records
Thiruvananthapuram - 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

IMPORTANT INFORMATION

1	Inviting Officer	The Director, Department of Survey and Land Records
2	Last date & time for submission of bid	23/01/2023 at 15.00 Hrs
3	Bid Submission Mode	Offline (In a sealed envelope)
4	The Bid Document, complete in all respects, to reach at the address , on or before the due date	Directorate of Survey & Land Records, Survey Bhavan, Vazhuthacadu, Thiruvananthapuram -14
5	Pre-Bid Meeting (Google Meet)	16/01/2023 at 12.00 Hrs Meet ID : meet.google.com/kbc-zxqc-egh
6	Date & time of opening of Bids	23/01/2023 at 15.30 Hrs
7	Venue for opening Bids	Directorate of Survey & Land Records, Survey Bhavan, Vazhuthacadu, Thiruvananthapuram -14

8	Earnest Money Deposit (Refundable)	Rs. 2,000/- (Two Thousand Only)
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 Survey and Land Records (hereinafter referred to as DSLR) on behalf of 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 selected based on the competitive bidding process. Submission of bids shall be deemed to have been done after careful reading and examination of the tender 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 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 of 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 shall 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. INSTRUCTIONS TO BIDDERS

a. Only CERT-IN empanelled agencies will be eligible to submit the bids.
b. An EMD of Rs 2000/- by way of Demand Draft from a scheduled or nationalized bank in favor of Director, Directorate of Survey & Land Records payable at Thiruvananthapuram shall be enclosed with the bid.
c. Tender documents shall be signed and stamped in all pages by the Bidder. The tender documents shall be enclosed in an envelope which is duly sealed and indicating the tender number, the name and address of the Bidder and superscripted the Description of work. The tender shall reach the office of the Director, Directorate of Survey & Land Records, Survey Bhavan, Vazhuthacadu, Thiruvananthapuram, Kerala -14 on or before 03:00 pm on 23/01/2023.
d. Submission of bids will be as per the time schedule stated in this document.
e. 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
f. Late bids will not be accepted.
g. All pages in the document that forms part of the bid should be signed by the authorized signatory of the Bidder.
h. Bid should accompany a covering letter duly signed by the authorised signatory of the Bidder.

i. The agency shall bear all costs associated with the preparation and submission of the bid.

j. 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 language.

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

l. The Bidder is not allowed to modify or withdraw the submitted 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 for 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, the 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. The vendor also ensures that 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 with 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 the agreement with CERT-India.

x. The vendor shall not subcontract any part of work assigned to it, to any other vendor/agency/organization 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. 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. Performance Security : As a condition precedent to execution of the Agreement, the Successful Bidder after the tender shall ensure submission of the requisite unconditional irrevocable Bank Guarantee, in the prescribed format within 21 days as a Performance Security for the services

to be performed under the resultant Agreement. The Bank Guarantee amount should be equivalent to 5% of the total value of the contract rounded to the nearest rupee and it should remain valid for a period of 60 days beyond the date of completion of all contractual obligations of the supplier.

xiii. 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.

xiv. 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

xv. The whole process of starting the audit by the vendor till issue of final audit certificate should be completed within 2 months

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

xvii. In addition the above conditions mentioned, The General Terms and Conditions of Form of Tender in the Annexure-2 of Store Purchase Manual, Kerala is also applicable for this tender.

xviii. For more details regarding this tender the Bidders can contact Section -B in Directorate of Survey and Land Records during the office hours on or before 23/01/2023, 11 AM.

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. Financial 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. Tender documents shall be signed and stamped in all pages by the Bidder. The tender documents shall be enclosed in an envelope which is duly sealed and indicating the tender number, the name and address of the tenderer and superscripted the Description of work. The tender shall reach the office of the Director, Directorate of Survey & Land Records, Survey Bhavan, Vazhuthacadu, Thiruvananthapuram -14 on or before 03:00 pm on 23/01/2023.

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 whatsoever. 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 the 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. The 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 event but before the expiry of the stipulated date of completion, the Contractor/Vendor must inform the Department in writing about the occurrence of Force Majeure event 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 Contractor/Vendor 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 the Government of Kerala and the

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

P. R. PUSHPA
Deputy Director
Directorate of Survey & Land Records
Thiruvananthapuram - 14

APPENDIX 1(A)

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

Web Application Scoping Sheet for Security Assessment		
S.No.	**Web Application Assessment Details**	**Description**
1	Web Application Name & Description	https://staging.entebhoomi.kerala.gov.in
2	Type of application Web/Application/ Mob/Rest / Thick / Thin instance to assesses & number of Application (s)	Web application
3	How many login systems to assesses?	3
4	How many static pages to assesses? (Approximate)	0
5	How many dynamic pages to assesses? (Approximate)	75
6	Do you need want role-based testing performed against this application?	Yes
7	Do you need want credentialed scans of web applications performed?	Yes
8	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	PostgreSQL
9	Authorization No. of roles & types of privileges for the different roles	Roles - 23 Privileges – 120
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	No
11	Is it a hybrid application?	No
12	Whether the application was security audited earlier? If so, please mention details.	No

13	Front-end Tool [Server side Scripts] (i.e. c++, J2eee, ASP, Asp.NET, JSP, PHP, etc.) – PHP	Java
14	Operating System Details (i.e.Windows-2003, Linux, AIX, Solaris, etc.)	Linux
15	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Apache + Spring boot 2.6
16	Total No. (Approximate) of Input Forms	500
17	Total No. of input field	1200
18	Total No. of login modules	2
19	Number of Web Services, if any	1
20	Number of methods in all web services ?	12
21	Number of URL's require to assesses ?	1 (https://staging.entebhoomi.kerala.gov.in/)
22	Is this REST /SOAP based Application	Web Application
23	Is it Thick or Thin Client Application	Web Application
24	Is this Applications is ERP/ Enterprised based App	No
25	Does the application has or proposed to have payment gateway integration? Please specify	No
26	Is Application hosted in Cloud ? If yes which under cloud provider private & others (Govt SDC)	SDC

APPENDIX 1(B)

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

Web Application Scoping Sheet for Security Assessment		
S.No.	**Web Application Assessment Details**	**Description**
1	Web Application Name & Description	**M.app Enterprises & A cloud platform for creating geospatial apps for your organization**
2	Type of application Web/Application/ Mob/Rest / Thick / Thin instance to assesses & number of Application (s)	thin and web
3	How many login systems to assesses?	
4	How many static pages to assesses? (Approximate)	
5	How many dynamic pages to assesses? (Approximate)	10
6	Do you need want role-based testing performed against this application?	
7	Do you need want credentialed scans of web applications performed?	
8	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	**Postgres Sql**
9	Authorization No. of roles & types of privileges for the different roles	As of now only two were there
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	**Yes https://staging.entebhoomigis.kerala.gov.in/management**
11	Is it a hybrid application?	
12	Whether the application was security audited earlier? If so, please mention details.	**NO**
13	Front-end Tool [Server side Scripts] (i.e. c++, J2eee, ASP, Asp.NET, JSP, PHP, etc.) – PHP	

14	Operating System Details (i.e.Windows-2003, Linux, AIX, Solaris, etc.)	**2019 windows server**
15	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	
16	Total No. (Approximate) of Input Forms	
17	Total No. of input field	
18	Total No. of login modules	Multiple
19	Number of Web Services, if any	
20	Number of methods in all web services ?	RESTful web services
21	Number of URL's require to assesses ?	https://staging.entebhoomigis.kerala.gov.in/Apps/?tenant=Infinity_tenant
22	Is this REST /SOAP based Application	Rest
23	Is it Thick or Thin Client Application	Thin
24	Is this Applications is ERP/ Enterprised based App	Enterprised based app
25	Does the application has or proposed to have payment gateway integration? Please specify	no
26	Is Application hosted in Cloud ? If yes which under cloud provider private & others (Govt SDC)	Yes & SDC

APPENDIX 2

FINANCIAL BID SUBMISSION FORM

FINANCIAL BID SUBMITTED TO THE DIRECTOR OF SURVEY AND LAND RECORDS 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