

Office of the Land Revenue Commissioner

Public Office Building , Thiruvananthapuram , 695033

Mail ID :- lrcommissioner@gmail.com

e-Office CRU ID :- cru.lrctvm@kerala.gov.in

No. LR/9958/2023-IT CELL 4

Date:06-11-2023

NOTICE INVITING FINANCIAL BIDS

FOR

ENGAGING SERVICE PROVIDER FOR SECURITY AUDIT OF THE

SOFTWARE

APPLICATIONS OWNED BY

LAND REVENUE DEPARTMENT, GOVT. OF KERALA

IMPORTANT INFORMATION

1	Inviting Officer	The Commissioner, Land Revenue, Public Office Buildings, Thiruvananthapuram
2	Last date & time for submission of bid	18.11.2023, 4:45 PM
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	itcelclr.revenue@kerala.gov.in
5	Pre-Bid Meeting (Web - Meet)	13.11.2023, 3 PM
	Password Info sharing window	

6	(for the password protected pdf file)	After the bid submission date and till 1 hr prior to the bid opening time.
7	Date & time of opening of Bids	20.11.2023, 3 PM
8	Venue for opening Bids	Video Conference Hall, O/o Commissioner of Land Revenue, Public Office Buildings, Thiruvananthapuram -33
9	Contact Person for Queries	Nodal Officer, State IT Cell (Revenue), Commissionerate of Land Revenue, Public Office Buildings, Thiruvananthapuram -33 Phone - 854761 0009
10	Period of Completion of Work from the date of award of work	The vendor shall provide the first audit report not later than 3 weeks from the date of receiving the work order.

1. INVITATION OF BID

The Commissioner of Land Revenue (hereinafter referred to as Commissioner or CLR) on behalf of the Land Revenue Department, Government of Kerala (hereinafter referred to as the Department) invites financial bids from CERT-In EMPANELLED INFORMATION SECURITY on AUDITING ORGANISATIONS hereinafter referred to as "Bidder" till the award of Contract and thereafter award of contract, referred to as "Vendor/Contractor/Supplier/Successful Bidder") for conducting Application Security Audits for the Software Applications owned by the Department for a

period of 3 years. The successful Bidder shall be finalised 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 conform 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

- Identify the application level vulnerabilities on applications hosted in a test site / production site based on the latest top 10 OWASP vulnerabilities
- On demand application scans
- An audit of the environment along with the application to ascertain any vulnerability in the environment where the application is hosted .
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Web server information security
- Malicious File Uploads
- 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 the solution.

- Follow a specific format for reports.
- Certify the applications / websites tested as “ Safe for Hosting” and in times if Electronic Payment Gateway Operators request to provide it in their format.
- Accept responsibility for declaring the websites / URLs / mobile applications free from known vulnerabilities
- 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 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 by the department 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

1. Only the CERT-In empaneled agencies and being operational in Kerala will be eligible to submit the bids.
2. The duly signed bids should be submitted via email to itcelclr.revenue@kerala.gov.in
3. Submission of bids will be as per the time schedule stated in this document.
4. In consideration of the bidder being allowed to quote for the work, s/he should keep the tender response/bid firm for a period of 90 days from the date of opening the bid or till the bids are decided whichever is earlier. During the firm period s/he will not be free to withdraw the bids.
5. Late bids will not be accepted.
6. All pages in the document that forms part of the bid should be signed by the authorized signatory
7. Bid should be accompanied with a covering letter duly signed by the authorised signatory of the bidder.
8. The agency shall bear all costs associated with the preparation and submission of the Bid.
9. 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 CLR shall be in English or in case in another language, they should be accompanied by an accurate translation in English language.

10. The prices shall be quoted in Indian Rupees (INR) only.
11. The bidder is allowed to modify or withdraw its submitted bid any time prior to the last date prescribed for receipt of bids.
12. Subsequent to the last date for receipt of bids, no modification of bids shall be allowed.
13. 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.
14. 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.
15. The audit, as mentioned above, has to be completed in time irrespective of the number of projects handed over to the successful bidder. In case of multiple projects, it is expected that the successful bidder shall deploy multiple teams to complete all the multiple projects within the given time frame.

7. GENERAL TERMS AND CONDITIONS

1. The Commissioner reserves the right to amend or cancel the bid invitation in part or in full without prior notice at any point of time.
2. The bid inviting authority or other sanctioning authority reserves the right to reject any bid or all the bids without citing any reason thereof.
3. If the Commissioner deems it appropriate to revise any part of this invitation or to issue additional clarifications for interpretation of provisions of this document, he/she may issue supplements to this bid invitation. Any such supplement shall be deemed to be incorporated by this reference to this document

4. The successful bidder shall provide the first audit report to the department not later than 3 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.
5. 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.
6. The vendor will be terminated from audit engagements for reasons such as dishonoring audit commitments or violating these terms and conditions, degradation of auditor's performance or incompetence to meet expectations or if empanelment at CERT-IN ceases.
7. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.
8. 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.
9. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.
10. The vendor shall not subcontract any part of work assigned to another vendor or engage non-employees to perform the work.
11. 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 organisation 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 organisation's premises/ network and/ or shared to anyone except the auditors, auditee organisation, CERT-In and any other authorised Government entity. Any audit data should be wiped out from the vendor's domain after any engagement.

12. 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.
13. 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
14. The whole process of starting the audit by the vendor till issues of final audit certificate should be completed within 2 months
15. The audit should conform to the guidelines specified for the purpose by Government of Kerala vide G.O.(MS) No.8/2019/ITD Dated, Thiruvananthapuram,22.04.2019
16. The vendor should execute the works awarded during the entire period of contract as per the rates quoted in the bid.

8. FINANCIAL TERMS AND CONDITIONS

1. The rates should be quoted against each parameter under this invitation, excluding GST
2. The parameters for quoting the rates are given in the table below.

BASIC SLAB			
Sl No.	Parameters of the organisation	Parameter Range	Cost
1	Static pages	Extends up to 1000 pages	
2	Dynamic pages	Extends up to 1000 pages	
3	Input forms	Extends up to 20 forms	
4	Input fields	Extends up to 40 fields	
5	User roles	Extends up to 30 roles	
6	Screens in mobile app	Extends up to 20 screens	

ADDITIONAL CHARGES in excess of BASIC SLAB		
Sl No.	Parameters of the organisation	Cost
1	Static pages - per static page	
2	Dynamic pages-per dynamic pages	
3	Input forms-per input forms	
4	Input fields-per block of 10 input fields	
5	User roles-per user roles	
6	Screens in mobile app-per screens in mobile app	

3. For Audit of each application, the empanelled agency will be shared 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 1 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 itcelclr.revenue@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 itcelclr.revenue@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 itcelclr.revenue@kerala.gov.in after the last date prescribed for the submission of bids till 1 hr prior to the bid opening time.
6. Department will not be responsible for receiving passwords after the date and time specified in the document or non receipt of the same due to any technical error.

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. Acceptance

of the bid rests with the purchase committee which does not undertake to accept the lowest or any particular bid.

2. The acceptance of the bid will be intimated to the successful bidder by the Commissioner through e-mail prior to expiry of the period of the bid validity.

11. PAYMENT TERMS:

1. No mobilisation advance shall be paid.
2. Billing will be in a half yearly cycle- the first bill should be submitted in the month of August of the particular year and the second bill on February of the same year.
3. The payment shall be released to the vendor on submission of Bills (invoices) in Triplicate addressed to The Commissioner, Land Revenue, Thiruvananthapuram.

12. RIGHT TO TERMINATE PROCESS

1. The Commissioner can terminate the bidding process at any time without assigning any reason. CLR makes no commitments, expressed or implied that this process will result in a business transaction with anyone.
2. 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

1. Riot or civil commotion
2. Earthquake, Flood, Fire, Tempest, Epidemics, Lightning or other natural physical Disaster, Quarantine restricts and Freight embargoes
3. 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.

2. 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 produces 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.

13. 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

16. ARBITRATION

In case any dispute or difference arising in connection with the Agreement the same shall be settled by mutual discussion between the parties. Any unresolved disputes, if persists, can be settled in the civil courts having jurisdiction in Trivandrum.

APPENDIX 1**FINANCIAL BID SUBMISSION FORM**

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

Bid Submitted by: <Organisation Name>

Date of Submission : <Date>

BASIC SLAB		
SI No.	Parameters of the organisation	Cost excluding GST
1	Static pages Extends upto 1000 pages	
2	Dynamic pages Extends upto 1000 pages	
3	Input forms Extends upto 20 forms	
4	Input fields	

4	Extends upto 40 fields	
5	User roles Extends upto 30 roles	
6	Screens in mobile app Extends upto 20 screens	
ADDITIONAL CHARGES in excess of BASIC SLAB		
7	Static pages - per static page	
8	Dynamic pages-per dynamic pages	
9	Input forms-per input forms	
10	Input fields-per block of 10 input fields	
11	User roles-per user roles	
12	Screens in mobile app-per screens in mobile app	

Total Cost in Figures :

Total Cost in Words: notice

Authorised Signatory

Dr A KOWSIGAN IAS, COMMISSIONER C L R, O/o Commissioner

CLR