Government of Kerala
Department of Electrical Inspectorate
Office of the Chief Electrical Inspector
Housing Board Buildings, Shanthi Nagar
Thiruvananthapuram 695 001
Phone: 0471 2330558 , 0471 2331104
Email : cei.kerala@kerala.gov.in,
ceikerala@gmail.com
Web site: www. dei.kerala.gov.in

भारतीय मानक ब्यूरो IS 15700
मानकः पथप्रदर्शक
BUREAU OF INDIAN STANDARDS SQMS
An IS 15700 : 2005 Certified Department

No. CEI/3510/2026-G1 Date: 25-10-2026

Quotation Notice -1

Sealed quotations are invited for the Security Audit of Suraksha Software.

Quotation Number	01/Qn/2026-27/CEI
Due date and time for receipt of quotations	30/10/2026 5.00PM
Date and time for opening of quotations	31/10/2026 11.00AM
Date up to which the rates are to remain firm for acceptance	3 months from date of opening of quotation.
Designation and address of the officer to whom the quotation is to be addressed	Chief Electrical Inspector, Department of Electrical Inspectorate, Govt. of Kerala, Housing Board Buildings, Santhi Nagar, Thiruvananthapuram – 1
Superscription	
Service delivery location	Office of the Chief Electrical Inspector, Housing Board Buildings, Santhi Nagar, Thiruvananthapuram – 1

Request for Proposal:-
Proposals are invited for the security auditing of the Suraksha Software developed for the Department with scope of work as specified below.

Scope of Work:-

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 of 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 conceding security audit related aspects; not essentially covered by work-areas outlined above.
- The selected vendor may cover the below mentioned tests for the application or website provided for testing:
- ***Application Security Audit***
- ***Penetration Testing***

- ***Vulnerability Testing***
- ***Database Server Controls***
- ***Physical Access Control***
- ***Network security Review as part of Application Security***
- ***Compliance Review***
- Black box testing for Security Audit should follow OWASP guidelines covering to 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

    - Audit shall cover all requirements specified in the Government Order GO (Ms) No 8/2019/ITD dated 22.04.2019.
    - Rate of service shall be as specified in the Government Order GO (Ms) No 8/2019/ITD dated 22.04.2019

Details of Web Application and Mobile Application to be assessed

Sl No	Assessment Details	Description
1	How many web application instance to assesses?	1
2	How many login systems to assesses?	Dynamic
3	How many static pages to assesses? (Approximate)	15
4	How many dynamic pages to assesses? (Approximate)	25
5	Do you need fuzzing performed against this application?	No
6	Do you need want role-based testing performed against this application?	Yes
7	Do you need want credentialed scans of web applications performed?	No
8	Back-end Database(MS-SQL Server, PostgreSQL,Oracle, etc.)	PostgreSQL
9	Authorization No. of roles & types of privileges for the different roles	Dynamic
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	No
11	Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) –PHP	PHP - Laraval
12	Operating System Details(i.e.Windows-2003, Linux, AIX, Solaris, etc.)	Ubuntu 20.04 LTS
13	Application Server with Version (i.e. IIS 5.0.Apache,Tomcat, etc.)	Apache
14	Total No. (Approximate) of Input Forms	12
15	Total No. of input field (Approximate)	150
16	Total No. of login modules	6
17	Number of Web Services, if any	45
18	Number of methods in all web services ?	30

19	Number of URL requires to assess	One
20	Application Type – REST/SOAP based	REST
	Mobile Application (Android and iOS)	
21	Number of screens in Mobile App	
22	Total No of input forms	12
23	Total No of input fields	150
24	Total No of parameters in API	90
25	Total No of user roles such as admin, manager user	8
26	Type of App such as native app or mobile web app or hybrid app	Hybid app
27	Technologies such as HTML, CSS, Java, PHP	Flutter-Dart
28	Back end web services and database	REST and PostgreSQL

Security Audit Scoping Sheet for Mobile and Web Applications

Field	**Details**
Department Name	Department of Electrical Inspectorate, Government of Kerala
Head of the Department	Chief Electrical Inspector
Office Address	Office of the Chief Electrical Inspector, Housing Board Building, Shanti Nagar, Thiruvananthapuram 695001
Nodal Contact Person	Rahul J S, Assistant Electrical Inspector
Nodal Officer's Contact Number	Mobile:9497486824 office number: 0471-2330558
Official Email ID	cei.kerala@kerala.gov.in

A. Common to all three phases

S.No.	**Item (same for all phases)**	**Answer**
2	Web Application URL	https://suraksha.ceikerala.gov.in/
3	Instances	1 web application instance, scoped here in three phases.
4	Login systems	3, shared. Public applicant, office staff, and KSWIFT.
7	Fuzzing	Yes.

8	Role-based testing	Yes. One public applicant and at least two office seats with different menus.
9	Credentialed scans	Yes. Department will give test accounts.
10	Back-end Database	PostgreSQL. One database for the website and the mobile app. Port 5432.
11	Roles and privileges	2 actor types: Public applicant and Office staff. Staff rights change by seat.
13	Server-side scripts	PHP (Laravel 9) and Blade. Browser: HTML, CSS, jQuery, Bootstrap, DataTables.
14	Operating system	Application requires PHP 8.x.
15	Application server	Apache with PHP. Framework: Laravel 9.
18	Login modules	3. Public, staff, and KSWIFT.
20	CMS	No third-party CMS.
22	REST / SOAP	Website is server-rendered PHP. Mobile API and partner calls are HTTP. Not SOAP.

B. Split by phase

Phase 1 has 19 dynamic pages, Phase 2 has 25, and Phase 3 has 35 web pages. Together that is 79 dynamic web pages, plus 3 static pages.

Item that differs	**Phase 1**	**Phase 2**	**Phase 3**
Functions counted as one page each	Dashboard, application status, profile, registration, scheme approval, sanction, completion report, line clearance, soil resistivity, valuation, MV addition, payment, and the office lists for scheme, line clearance, soil, valuation, plus administration.	Temporary connection, lift permit, lift sanction, cable TV, VIP visit, lift manufacturer, cinema and D certificate, D-certificate renewal, lift renewal, manufacturer renewal, accident complaint, grievance, lift completion report, and the office lists for those services plus periodical schedule, tour, demanding, and invoice.	Unauthorized connection, lab application, lab list, job register, lab reports, feedback, lab categories, lab staff, inventory (6 menus), assets (6 menus), electricity duty (5 menus), quality control (9 menus).
5. Static pages	3. Home, FAQ, and Privacy policy. Counted once, here.	None.	None.
6. Dynamic pages	19. One page per function. Opening a file, its history, a pop-up, or a printout is the same function, not another page.	25. One page per Phase 2 service form or office list. Cinema operator and AC check are inside the cinema screen, not a separate page.	35 web pages. One page per menu function. Detail and pop-up screens are not added again. Mobile is in section C.
16. Input	49 forms on those 19	65 forms on those 25 pages.	36 forms on those 35

forms	pages.		web pages.
17. Input fields	421 fields on those 19 pages.	637 fields on those 25 pages.	287 fields on those 35 web pages.
19. Web services	SWIFT, eTreasury, and KSWIFT. About 48 API routes.	No API of its own. Payment uses eTreasury from Phase 1.	Mobile API, 21 routes. The other Phase 3 modules are website menus.
20. API methods	About 48 HTTP operations.	None of its own.	21 mobile API operations.
21. URLs to assess	3 static + 19 dynamic pages.	25 dynamic pages.	35 web pages and 15 mobile screens.

C. Mobile application - Phase 3 only

Android and iOS are the same app, so the figures are written once. Phase 1 and Phase 2 have no mobile app.

S.No.	Android and iOS (same app)	Details
1	Screens	15 screens a user can open.
2	Input forms	4. Login, profile, change password, OTP.
3	Input fields	8.
4	API parameters	16, plus the access token.
5	User roles	2. Public and office staff.
6	Type of app	Native Flutter 1.0.0. One project for Android and iOS.
7	Technologies	Flutter / Dart. Calls the PHP API.
8	Backend and database	/api/mobile/v1 on the same site. PostgreSQL.

Other Terms and conditions for compliance by the vendors:

The acceptance of the proposal will be subject to the following conditions:

1. Proposal shall be submitted on or before 30/10/2026 at 5PM. Proposals received after cutoff date will not be considered.
2. The bidder should be a CERT-IN empaneled or Government approved security auditing form.
3. For security auditing of Government assets, the vendor shall not Charge cost exceeding the rates finalized by the Government.
4. The vendor shall conduct a pre-assessment to understand the audit requirements of the organization/Department and shall provide the draft scope of work in detail at free of cost, if requested by the department.
5. The vendor shall provide the first audit report not later than 3 weeks from receiving the work order. Subsequent interim reports shall be issued not later than 8 working days of receiving the patched application for re-test.

6. 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 user 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.

7. 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-India ceases.

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

9. 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 hand holding on how to fix the issues.

10. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.

11. The vendor shall not sub contract any part of work assigned to another vendor or engage non-employees to perform the work.

12. 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-ln and any other authorized Government entity. Any audit data should be wiped out from the vendor’s domain after any engagement.

13. 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 hosting Service provider before issuing the audit certificate.

14. The vendor shall provide any audit report or data as required by KSITM with respect to audits perfumed for Government of Kerala.

15. Withdrawal from the proposal after it is accepted or failure to service within a specified time or according to specifications will entail cancellation of the order and purchases being made at the officer’s expenses from elsewhere, any loss incurred thereby being payable by the defaulting party. In such an event the Government reserves also the right to remove the defaulter’s name from the list of Government suppliers permanently or for a specified number of years.

16. No representation for enhancement of price once accepted will be considered during the period of the contract.

17. Any attempt on the part of tenderers or their agents to influence the Officers concerned in their favor by personal canvassing will disqualify the tenderers.

18. If any license or permit is required, tenderers must specify in their proposal and also state the authority to whom application is to be made.

19. Any sum of money due and payable to the contractor (including Security Deposit returnable to him) under this contract may be appropriated by the Purchasing Officer or Government or any other person authorized by Government and set-off against any claim of the Purchasing Officer or Government for the payment of a sum of money arising out of or under any other contract made by the contractor with the Purchasing officer or Government or any other person authorized by Government.

20. The prices quoted should be inclusive of all taxes, duties, cesses, etc., which are or may become payable by the contractor under existing or future laws or rules of the country of origin/supply or delivery during the course of execution of the contract.

21. Process of procurement will be as per the conditions mentioned in GO (Ms) No 8/2019/ITD dated 22.04.2019. 50% payment will be paid on submission of first Audit report and remaining payment will be released only after issue of the final audit report and Security Audit Certificate.

22. Any sum of money due and payable to the successful tenderer or contractor from Government shall be adjusted against any sum of money due to Government from him under any other contracts.

23. Special conditions, if any, printed on the proposal sheets of the tenderer or attached with the tender will not be applicable to the contract unless they are expressly accepted in writing by the purchases.

Digitally signed by
RAJESH BABU R
Date: 25-10-2026
10:59:53

Chief Electrical Inspector

1. Notice Board / Website

2. Spare