REC POWER DISTRIBUTION ISO 9001:2015, ISO 14001 : 2015 & OHSAS 18001 : 2007 Certified Company

आरईसी पावर डिस्ट्रीब्यूशन कम्पनी लिमिटेड
REC POWER DISTRIBUTION COMPANY LIMITED
(A wholly owned subsidiary of REC Ltd., a 'Navratna CPSE' under Ministry of Power, Govt. of India)
CIN No. RECPDCL-U40101DL2007GOI165779
Corporate Office: 4th Floor, KRIBHCO Bhawan, A-10, Sector-1, Noida, Gautam Budh Nagar - 201301 (UP)
Tel: 0120-4383783 Fax: 120-4383768, Website: www.recpdcl.in, E-mail: co.delhi@recpdcl.in
Regd. Office: Core-4, SCOPE Complex, 7 Lodhi Road, New Delhi-110003, Phone: 011-43091500 Fax: 011-24360644

सौभाग्य

RECPDCL/IT/ITSEC/2018/4170 Date: - 22/11/2018

To,
As per list attached (**Annexure- III**)

Sub: - Inviting quotation for engage CERT-IN empanelled security auditing agency to conduct security audit of SAUBHAGYA Web Application including Web Services and Mobile application.

Dear Sir,

REC Power Distribution Company Limited (REC PDCL) an ISO 9001:2015, ISO 14001:2015 & OHSAS 18001:2007 Certified Company, a wholly owned subsidiary of REC Ltd., a 'Navratna' CPSE under Ministry of Power, intends to conduct a security audit of its SAUBHAGYA web and mobile application through a CERT-IN empanelled security auditing agency of DeitY, Ministry of Communication & IT, Govt. of India are registered in Delhi/NCR. The objective of this audit is to assess security vulnerabilities as per the latest standards and reduce the risk.

The detailed objective & deliverables of the Security audit is enclosed as Annexure – I and the scope of work enclosed as Annexure - II. As your company is CERT-In emplaned agency as per the information available in CERT-In website (http://www.cert-in.org.in/PDF/Empanel_org.pdf) you are requested to send your quotation as per the following format.

S. No.	Description	Amount (in Rs.)	Taxes (if any)	Total Price (in Rs.) (inclusive of taxes)
1	Lump sum amount to Complete all levels of Security Audit of SAUBHAGYA Web Application including Web Services & Mobile Application in Android platform with Report Generation, recommendations and issue a Security Clearance Certificate. (As per scope of work & deliverables at Annexure I & II)			
GRAND TOTAL				

Terms & Conditions:

1. The price bids of those firms will be opened who fulfils the terms and conditions.
2. Only those Organizations/firms registered with the CERT-in-empanelled in Delhi/NCR are eligible for submitting the quotation.
3. Incomplete or conditional quotation will not be entertained.
4. No quotation will be accepted after closing date and time.
5. The agency will be removed from empanelment if due to any reason CERT-In has removed or not extended the empanelment of the agency.
6. The selected agency will not outsource any activity to other agency.
7. The selected agency will maintain confidentiality of the findings of security audit and ensure that the findings and corrective actions are shared with concerned stake holders of the project

8. **Schedule**: The first round of Web Application including Web Services & Mobile Application in Android platform audit report should be submitted to RECPDCL within 10 days after the work order issued by RECPDCL and consecutive round report if any, should be submitted within 5 days.
9. The bidder may remain present himself /herself or his/her authorized representative at the time of opening the quotation.
10. Any firm/organization blacklisted by a Govt./Semi Govt. Deptt. shall not be considered for this bid and bid will be rejected straightway.
11. A copy of terms & conditions attached as and Scope of work attached as duly signed by the tenderer, as a token of acceptance of the same should be attached along-with the tender.
12. The Tender Committee reserves the right to relax any terms and condition in the Govt. interest, with the approval of competent authority.
13. All disputes are subject to the jurisdiction of the Courts in the N.C.T. of Delhi.
14. Prices should be indicated in Indian Rupees only and in the respective units indicated at each row.
15. Calculations against each row as specified in the price schedule should be carried out carefully both for the total of each row and the Grand Total. Furnishing of any miscalculation etc. shall be at the bidder's risk and cost and the bid may be liable for summary rejection.
16. **Payment Terms:** 100% payment will be made only after submitting the final security audit certificate on completion of Audit of SAUBHAGYA Web Application including Web Services & Mobile Application in Android Platform.
17. Under no circumstances any extra/ additional taxes, duties, levies etc. shall be payable to the bidder by RECPDCL unless such a tax, duty or levy has been newly introduced and notified by the Government of India.
18. The bidder shall be the single point of contact for RECL till the completion of audit process.
19. **Penalty Clause:**
    a. Failure to complete the audit along with deliverables on or before the stipulated date will entail a penalty equal to 1% of the value of the contract price per week / part their of subject to maximum of 10 % of total contract value.
    b. In case of delay in compliance with the order beyond 15 days of the stipulated time period, RECPDCL have right to cancel the order.

NOTE: DOCUMENTS REQUIRED TO BE ATTACHED WITH BID

1. Copy of GSTIN Registration and PAN.
2. Copy of authorization with CERT-in empanelment.
3. Copy of terms and conditions duly signed with seal of the firm/organization, in token of acceptance of terms and conditions.
4. Bidder should submit undertaking letter to this effect for single point of contact.

You are requested to quote your best rates as offered to the Government organisations in a sealed cover indicating "COMMERCIAL BID FOR CONDUCTING THE SECUIRTY AUDIT OF SAUBHAGYA WEB & MOBILE APPLICATION" addressed to the undersigned to reach on or before 03.12.2018, 11:00 hrs. (Address: 4th Floor, KRIBHCO Bhawan, A-10, Sector-1, Noida (UP)-201301) and submitted sealed quotation will be open on 03.12.2018 at 12:00 hrs. (on same day).

-Sd-
(Bhupender Gupta)
Addl. CEO

Objectives:

1. To conduct security audit to assess vulnerabilities to the Web application including Web Services & Mobile application in Android Platform as per the ISO standards and OWASP top 10 vulnerabilities (Web & Mobile). The audit shall be conducted to review the intent and vulnerabilities to the organisations SAUBHAGYA application.
2. Security Audit is intended to give developers and security teams the resources they need to build and maintain secure mobile & web applications. Through the project, our goal is to classify security risks and provide developmental controls to reduce their impact or likelihood of exploitation.
3. To identify the vulnerabilities present in the SAUBHAGYA mobile and web application.
4. To identify the corrective measures and rectification of the vulnerabilities in mobile and web application.

Deliverables:

- The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.
- The agency should provide support to the development team for changes in coding to remove the vulnerabilities.
- Vulnerability Assessment Report, Penetration Test Report.
- Compliance review should be done after ensuring that changes to remove the vulnerabilities are completed by the development team.
- Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application or website has no vulnerabilities as a result of changes done in the code
- 1 day training session on the security for – No. of participants to also cover facilitation for closure of audit findings.

The proposed scope of work

A. <u>Audit of the SAUBHAGYA Web Application including Web Services and Mobile application in Android platform:</u>

1. The Applications Security audit has to be done on the following parameters -
   - To Assess Flaws in the Design of the Applications.
   - Attempting to guess passwords using password-cracking tools.
   - Validations of various data inputs.
   - Exception handling and logging.
   - Logical access control and authorization.
   - Evaluate the environment under which the application runs.
   - An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.
   - Malicious modification of data.
   - To assess the security between Web and Mobile Application
   - Application Security Audit
   - Penetration Testing
   - Vulnerability Testing
   - Compliance Review
2. Checking if commonly known holes in the software exist.

3 SAUBHAGYA Web application including Web Services and Mobile application in Android platform should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) for both Web & Mobile and Web Services (refer table 6.1 & 7.1).

4 The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Portal "Certified for Security".

5 Auditor must test Web application including Web Services and mobile application in Android platform for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to application.

- ✓ Vulnerabilities to SQL Injections
- ✓ CRLF injections
- ✓ Directory Traversal
- ✓ Authentication hacking/attacks
- ✓ Password strength on authentication pages
- ✓ Scan Java Script for security vulnerabilities
- ✓ File inclusion attacks
- ✓ Exploitable hacking vulnerable
- ✓ Web server information security
- ✓ Cross site scripting
- ✓ PHP remote scripts vulnerability
- ✓ HTTP Injection
- ✓ Phishing a website
- ✓ Buffer Overflows, Invalid inputs, insecure storage etc.
- ✓ Any other attack that can be a vulnerability to the website or web applications.

6 *The Top 10 Web application security vulnerabilities, which are given below, should also be checked, but not restricted to the following. The best practices in the industry must be followed.*

6.1- Top Ten Most Critical Web Application Security Vulnerabilities		
A1	**Injection**	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	**Broken Authentication**	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3	**Sensitive Data Exposure**	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4	**XML External Entities (XXE)**	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6	**Security Misconfiguration**	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7	**Cross-Site Scripting (XSS)**	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8	**Insecure Deserialization**	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9	**Using Components with Known Vulnerabilities**	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a

		vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10	**Insufficient Logging & Monitoring**	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

7 *The Top 10 Mobile application security vulnerabilities, which are given below, should also be checked, but not restricted to the following. The best practices in the industry must be followed.*

7.1 - Top Ten Most Critical Mobile Application Security Vulnerabilities		
M1	**Improper Platform Usage**	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2	**Insecure Data Storage**	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3	**Insecure Communication**	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc
M4	**Insecure Authentication**	This category captures notions of authenticating the end user or bad session management. This can include: Failing to identify the user at all when that should be required Failure to maintain the user's identity when it is required Weaknesses in session management
M5	**Insufficient Cryptography**	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
M6	**Insecure Authorization**	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.
M7	**Client Code Quality**	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
M8	**Code Tampering**	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

		Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
M9	**Reverse Engineering**	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
M10	**Extraneous Functionality**	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

7.2 Auditor must test Malicious Functionality & Vulnerabilities in Mobile Application

- Activity monitoring and data retrieval
- Unauthorized dialing, SMS, and payments
- Unauthorized network connectivity (exfiltration or command &
- control)
- UI Impersonation
- System modification (rootkit, APN proxy config)
- Logic or Time bomb
- Sensitive data leakage (inadvertent or side channel)
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Hardcoded password/keys

8 Auditor to test vulnerabilities in Web Services as per Industry practices/OWASP.

B. <u>Audit Report</u>

The Web application including Web Services and Mobile application in Android platform security audit report is a key audit output and must contain the following:

1. Identification of Auditee (Address & contact information)
2. Dates and Location(s) of audit
3. Terms of reference (as agreed between the Auditee and Auditor), including the standard for Audit, if any.
4. Audit plan.
5. Additional mandatory or voluntary standards or regulations applicable to the Auditee.
6. Audit Standards should be followed.
7. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
   i) Tools used
   ii) List of vulnerabilities identified
   iii) Description of vulnerability
   iv) Risk rating or severity of vulnerability

v) Test cases used for assessing the vulnerabilities
vi) Illustration if the test cases to provide the vulnerability
vii) Applicable screen dumps

8. Analysis of vulnerabilities and issues of concern.
9. Recommendations for action.
10. Personnel involved in the audit.

The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

Annexure- III

CERT-In Empanelled Agencies registered offices in Delhi/NCR

1. M/s AKS Information Technology Services Pvt. Ltd.,
   E-52, Sector-3,
   Noida – 201301 (UP)
   Website URL : http://www.aksitservices.co.in
   Ph: 0120-4545911, 0120-2542253 Fax: 0120-4243669
   Contact Person: Mr. Ashish Kumar Saxena, Managing Director
   Mobile: +91 7290058951 E-mail: info.cert[at]aksitservices.co.in 4. M

2. M/s ALLIED BOSTON CONSULTANTS INDIA PVT. LTD
   2205, Express Trade Towers 2,
   Sector 132, Noida - 201301, INDIA
   Ph : +91-120-4113528 / 4113529
   Contact Person: Mr. T. GANGULY
   E-mail: t.ganguly[at]abcipl.co.in

3. M/s Cyber Q Consulting Pvt Ltd.
   622 DLF Tower A, Jasola
   New Delhi-110044
   Website URL: http://www.cyberqindia.com
   Ph: 011-41077560 Fax: 011-41077561
   Contact Person: Mr. Debopriyo Kar, Head-Information Security
   Mobile: +91 9810033205 / 9968846947 E-mail: debopriyo[dot]kar[at]cyberqindia.com

4. M/s CyberRoot Risk Advisory Pvt. Ltd.
   901 and 902, 9th Floor, JMD Regent Square,
   MG Road, Gurgaon -122002, Haryana
   Contact Person: Vijay Singh Bisht, Managing Director
   Email: cert[at]crriskadvisory.com Mobile: +91-9210000117

5. M/s Esec Forte Technologies Pvt Ltd
   Corporate Office (Mailing Address): Level 2, Enkay Centre, Vanijya Kunj,
   Udyog Vihar, Phase - V, Gurgaon -122016 (Opp. Cyber Hub)
   Tel: +91 124 4264666, +91 9871699555
   Contact Person: Mr. Kunal Bajaj, Chief Business Officer
   Mobile : +91- 9871699555 E-mail : kunal[at]esecforte.com

6. M/s Grant Thornton India LLP
   L 41, Connaught Circus, Outer Circle, New Delhi. PIN - 110 001
   Ph : 0124-4628000 (Ext. 277) Fax: +91 124 462 8001
   Contact Person : Mr. Prashant Gupta
   Mobile:+91 9958882282 E-mail :Prashant.Gupta[at]IN.GT.COM

7. M/s HCL Comnet Ltd
   A-104, Sector 58, Noida - 201301
   Ph: 0120-4362800 Fax: 0120-2539799
   Contact person : Mr. Sreekumar KU, AVP
   Mobile : +91 9650263646 E-mail : sreekumarku[at]hcl.com

8. M/s KPMG
   8th floor, Tower B, DLF Cyber City,
   Phase-II, Gurgaon- 122002
   Website URL: www.kpmg.com
   Ph : 0124-3074134 Fax: 0124-2549101
   Contact Person: Mr. Atul Gupta, Director
   Mobile : +91 09810081050 E-mail : atulgupta[at]kpmg.com

9. M/s Lucideus Tech Private Limited
   NSIC Campus, Software Technology Park Extn,
   Okhla Phase III, New Delhi - 110020
   Contact person:Mr. Srivathsan Sridharan, Vice President- Sales
   Mobile: 9599057764 Email: sri.s[at] lucideustech.com

10. M/s Mahindra Special Services Group
    212, 2nd Floor, Rectangle One,
    Commercial Complex D4, Saket, New Delhi-110017
    Ph: 022-24984213 Fax: 022-24916869
    Contact person :Mr. Dinesh K Pillai, Chief Executive Officer
    Mobile : +91 9769693764 E-mail : dinesh.pillai[at]mahindrassg.com

11. M/s Maverick Quality Advisory Services Private Limited
    123 RADHEY SHYAM PARK P.O SAHIBABAD
    Ghaziabad, U.P, INDIA – 201005
    Ph :9871991928
    Contact Person : Ashok Vardhan,Director
    E-mail :ashok[at]mqasglobal.com

12. M/s PricewaterhouseCoopers Pvt Ltd
    Building 8, 7th & 8th floor, Tower- C,
    DLF Cyber city, Gurgaon- 122002
    Website URL: www.pwc.com/in/en
    Ph : 0124-4620000 Fax: 0124-4620620
    Contact Person: Mr. Rahul Aggarwal, Director
    Mobile : +91 09811299662 E-mail : Rahul2.aggarwal[at]in.pwc.com

13. M/s Panacea InfoSec Pvt Ltd.
    226, Pocket A2, Pocket B,
    Sector 17 Dwarka, Dwarka, Delhi, 110075
    Mobile Number: 1- +91-9650028323 (Prefered) - Apurva 2- +91-9810944187 (Alternative) – Ajay 3- +91-7007246077 (Alternative) - Chandani Landline Number: +91 11 49403170 (Office) Contact E-mail : 1- apurva[at]panaceainfosec.com 2- ajay[at]panaceainfosec.com 3- cg[at]panaceainfosec.com

14. M/s Protiviti India Member Private Limited
    15th Floor, Tower A, Building No 5,
    DLF Phase III, DLF Cyber City, Gurgaon-122002, Haryana, India
    Ph: +91 9821229027
    Contact Person: Nikhil Donde (Managing Director)
    E-mail: nikhil.donde[at]protivitiglobal.in

15. M/s Recon Business Advisory Pvt. Ltd.
    Shree Capt. Satya Yadav , CEO & MD F-8, 3rd Floor,
    Kalkaji Main Road, New Delhi - 110019.
    Contact Person: Ankush Batra (Director)
    Email: cert[at]reconglobal.in / accounts[at]reconglobal.in
    Mob: 9205019013 Web: www.reconglobal.in

16. M/s STQC Directorate
    Electronics Niketan, 6 CGO Complex,
    Lodhi Road, New Delhi- 110003
    Website URL: www.stqc.gov.in Ph : 011 24301816 Fax: 011 24363083
    Contact Person: Mr. Aashish Banati, Scientist 'F',
    E-mail : abanati[at]stqc.gov.in Mobile: 9968314724

17. M/s Sandrock eSecurities Pvt Ltd
    E-46, Rani Garden Extension, Shastri Nagar, Delhi - 110031
    Contact Person: Rachna Agarwal, Head – Business Operations
    Mobile: 9560211616 Email: pentest[at]sandrock.in

18. M/s Torrid Networks Private Limited
    C-171, 2nd Floor, Sector-63
    Noida-201301 Uttar Pradesh
    Ph: +91-120-4270305, +91-120-4216622 Fax: 012-04235064
    Contact Person :Mr. Salil Kapoor
    Mobile : + 91 92 666 666 91 E-mail : apac[at]torridnetworks.com

19. M/s Trusted Info Systems Private Ltd.
    B-4, GF, Kailash Apartment, (Near Kailash Colony Metro station, Opp Metro Pillar 71)
    Lala Lajpat Rai Marg, New Delhi - 110048
    Ph: 91-011-29248058
    Contact Person : Vijender Kaushik
    Mobile :+91-9810259365 E-mail : vijender.kaushik[at]trustedinfo.com

20. M/s Wipro Ltd
    Wipro Infotech, 480-481, Udyog Vihar,
    Phase-III, Gurgaon, Haryana
    Ph No: 0124-3084000 Fax : 0124-3084269
    Contact Person : Mr. Prabir Kumar Chaudhuri
    Mobile : +91 9818600990 Fax: 0124-3084269 E-mail : prabir.chaudhuri [at]wipro.com

21. M/s Xiarch Solutions Pvt Ltd
    352, 2nd Floor Tarun Enclave, Pitampura, New Delhi-110034
    Ph: 011-45510033 Fax:011-66173033
    Contact Person:Utsav Mittal, Principal Consultant
    Email: utsav[at]xiarch.com / cert[at]xiarch.com Mobile :9810874431