REC Power Development and Consultancy Limited
(Formerly Known as REC Power Distribution Company Limited
A wholly owned subsidiary of REC Limited, a 'Navratna CPSE'
under Ministry of Power. Govt. of India)

No. RECPDCL/Tech/Audit/ 2021-22/1248 **Dated: 09.09.2021**

Notice Inviting Limited Tender

(**Invited through e-Tendering mode only**)

GeM Availability Report ID: GEM/GARPTS/14072021/8EEN2UFP595I

Limited to Agencies as per list enclosed as FORM-VIII

To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application.

Important Dates	
Date of Release of Limited Tender	09.09.2021
Last date of submission of Limited Tender	24.09.2021
Date of Opening of Financial Bid	**To be intimated later**

Corporate office
REC Power Development and Consultancy Limited
D Block, REC World Head Quarter,
Plot No. I-4, Sector-29, Gurugram, Haryana-122001
Website: **www.recpdcl.in**

Description of Task, e-tender submission format and procedure is provided in the NIT document available on RECPDCL website **(www.recpdcl.in)**, REC website **(www.recindia.nic.in),** e-tendering website **(www.tenderwizard.com/REC),** Central Public Procurement Portal **(www.eprocure.gov.in)**

Note: Online registration has to be done at e-tendering website i.e. **www.tenderwizard.com/REC** & in general; activation of registration may take about 24 hours subject to the submission of all requisite documents required in the process.

-Sd-
(S S Gupta)
Addl. C.E.O.

INDEX

SECTION-I
(TENDER INFORMATION)

Name of the assignment:

To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application

Important information

S. No	Event	Date/ Information
1	Date of Release of Limited Tender	**09.09.2021**
2	Last date for queries / seeking clarification	**13.09.2021 up to 17:00 Hrs**
3	Pre Bid Meeting	**15.09.2021 at 11:30 Hrs**
4	Last date of submission of Limited Tender	**24.09.2021 up to 15:00 Hrs**
5	Date of Opening of Technical Bid(s)	**24.09.2021 at 15:30 Hrs**
6	Date of Opening of Financial Bid(s)	**To be intimated later**
6	Bid document	The Bid document can be downloaded and viewed from any of the website: **www.recpdcl.in** (or) **www.recindia.nic.in** (or) **www.eprocure.gov.in** (or) (**www.tenderwizard.com/REC**) at free of cost.
7	Validity of Bid	90 days from the last date of bid submission
8	Earnest Money Deposit (EMD)#	Not Applicable

8	Address for Bid Submission	**Shri Shambhu Shanker Gupta,** Addl. Chief Executive Officer, REC Power Development and Consultancy Limited, D Block REC World Head Quarter, Plot No. I-4, Sector-29, Gurugram, Haryana-122001 **Email**: co@recpdcl.in & urjamitra@recpdcl.in
9	Contact Person	**Shri Ankit Kumar,** CM (Tech) and/or **Shri Manish Kumar Singh**, DM (Tech) REC Power Development and Consultancy Limited, D Block REC World Head Quarter, Plot No. I-4, Sector-29, Gurugram, Haryana-122001 **Email**: co@recpdcl.in & urjamitra@recpdcl.in

The bidders are exempted from submission of EMD. However, a declaration in this regard as per attached format is required to be uploaded while submitting the financial bid in line with guideline issued by Department of Expenditure, Ministry of Finance, Govt. of India.

SECTION-II

INSTRUCTIONS TO AGENCIES

SUBMISSION PROCESS OF BID DOCUMENTS:

A. Downloading & viewing of Tender Document:

Bidders can download and view tender document from RECPDCL web site **www.recpdcl.in** (or) e-tender website **www.tenderwizard.com/REC** (or) REC website **www.recindia.nic.in** (or) Central Public Procurement Portal **www.eprocure.gov.in** at free of cost.

B. Participation through e-Bid Submission:

Bidders shall submit their Financial Bid documents online through website www.tenderwizard.com/REC

1) In order to participate in e-Bid submission, it is mandatory for agencies to have log-in User ID and Password. For this purpose, the agency has to register with RECPDCL through tender Wizard website as per procedure given below.

   Steps for Online Registration:

   (i) Go to website https://www.tenderwizard.com/REC
   (ii) Click the link 'Register Me'
   (iii) Enter the details about the E-tendering as per format
   (iv) Click 'Create Profile'
   (v) System will provide / confirmation with Login ID and Password

   Note:

   - While accessing tenderwizard.com website, please type 'REC' in capital letters only to get access of e-tender portal.
   - Activation of On-Line registration may take about maximum 24 hours. It is the responsibility of the bidder to register in advance.

2) Please note that the agencies have to obtain digital signature token for applying the bid. Bidders may also obtain the same from Tender Wizard.

   Steps for applying for Digital Signature from Tender Wizard:

   - Download the Application Form from the website https://www.tenderwizard.com/REC. Follow the instructions as provided therein.

- In case of any assistance, you may contact RECPDCL officials whose address is given in this tender document, the bidders may also contact at Tender Wizard helpdesk numbers given in Contact Us section in the e-tendering portal www.tenderwizard.com/REC.

C. Submission of Bid Documents:

Submission of bids will be through **online e-tendering mode only from www.tenderwizard.com/REC website.**

Agencies should upload Bid documents (scanned copies) as mentioned below. Online submission of Bid documents is mandatory.

1) **Letter for Submission of Financial Bid** has to be submitted on Company's letterhead duly signed and stamped as per format of **Form-I**. This is mandatory document for submission.
2) **Bidder's General Details** has to be submitted on Company's letterhead duly signed and stamped as per format of **Form-II**.
3) **Letter for Transmittal** has to be submitted on Company's letterhead duly signed and stamped as per format of **Form-III**.
4) Undertaking towards not being blacklisted as per format of **Form-IV.**
5) **Financial Bid** has to be submitted **through online** mode **only** as per format of **Form-V**.
6) **Earnest Money Deposit Declaration as per Form-VI.**
7) Copy of GSTIN Registration and PAN.
8) Copy of authorization with CERT-in empanelment.
9) Copy of Tender documents duly signed with seal of the firm/organization, in token of acceptance of terms and conditions.
10) Bidder should submit undertaking letter to this effect for single point of contact.

Note: All the documents should be addressed to.

Addl. Chief Executive Officer
REC Power Development and Consultancy Ltd.
D Block REC World Head Quarter, Plot No. I-4, Sector-29, Gurugram, Haryana-122001

*(**Note:** All papers that comprise the Bid document of the concerned Bid must be numbered. An index of each page should also be provided)*

SECTION-III

DETAILED SCOPE OF WORK

The proposed scope of work:

A. Audit of the URJAMITRA Web Application including Web Services and Mobile application in Android and IOS platform:

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 exists.

3 URJAMITRA Web application including Web Services and Mobile application in Android & iOS 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). URL link for web and Mobile application are as below;

a) Urja Mitra web link: https://www.urjamitra.com/

b) Urja Mitra iOS link:

https://apps.apple.com/in/app/urja-mitra/id1173378490

c) Urja Mitra android link:

https://play.google.com/store/apps/details?id=map.googlemap.com.rec

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 & iOS platform for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to application.

- Vulnerabilities to MySQL Injections
- MySQL stored procedure injection
- 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
- JAVA remote scripts vulnerability
- HTTPS Injection
- RESTful web service API
- Phishing a website
- Buffer Overflows, Invalid inputs, insecure storage etc.
- Any other attack that can be a vulnerability to the website or web applications and the Mobile application (Android & iOS)

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 MySQL, 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 when ever 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 websites, 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 200days, 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/iOS intents, platform permissions, misuse of Touch ID, the Keychain, or some other security control that is part of the mobile operating
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, clear text 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, Hoppero tool, 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 (ex filtration or command & control)
- UI Impersonation

- System modification (root kit, 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 Urja Mitra Web application including Web Services and Mobile application in Android & iOS platform as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project).

9 Server(s) required for carrying out the audit of the URJAMITRA Web Application including Web Services and Mobile application shall be in the scope of the bidder. The bidder shall be responsible for arranging the Server (s) from for the entire duration of the contract, till issuance of the security clearance certificate.

10 The configuration of the production server of Urja Mitra application is: 1 VM (Application and database), 16vCPU, 64GB RAM, 500 GB Database and 50 GB Application (approx.), Linux (RHEL). The test Server(s) required for carrying out the audit of the URJAMITRA Web Application including Web Services and Mobile application shall be arranged with adequate configuration by the bidder.

11 The Urja Mitra application has 32 modules (approx.), 165 nos (approx.) dynamic pages, 177 nos (approx.) static pages and 53 nos (approx.) Web Service/API included in the existing web application & 40 nos (approx.) screens each for Android & iOS mobile application which has to be audited under the present scope of work.

12 **Audit Report**

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

i. Identification of Auditee (Address & contact information)
ii. Dates and Location(s)of audit
iii. Terms of reference (as agreed between the Auditee and Auditor), including the standard for Audit, if any.
iv. Audit plan.
v. Additional mandatory or voluntary standards or regulations applicable to the Auditee.

vi. Audit Standards should be followed.
vii. 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
    viii) Analysis of vulnerabilities and issues of concern.
    ix) Recommendations for action.
    x) 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.

10. Confidentiality

All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner, by the Auditor.

The selected agency shall submit the Model Non-Disclosure Agreement in the format as prescribed in Form VII in two (2) originals. The selected agency shall submit the Model Non-Disclosure Agreement on non-judicial stamp paper of Rs. 100/- each duly purchased from the National Capital Territory of Delhi.

SECTION – IV

Terms & Conditions

1. The bidder must be an empanelled auditor of CERT-In, having a valid CERT-In empanelment certificate on the date of tender publication. Copy of authorization with valid CERT-In empanelment certificate to be furnished.
2. Documentary evidence of firm's GST Registration shall be furnished. Bids not accompanied by the requisite documentary proofs shall be rejected.
3. Bids shall remain valid for 90 days from the date of Bid Opening. Any Bid valid for a shorter period than the period specified shall be rejected as nonresponsive.
4. Last date & Time for receipt of Bids: The last date for receipt of Bids is **24.09.2021** till **15**:**00 Hrs**. Bids will be opened on the same day at **15**:**30 Hrs**.
5. Submission of Bids: The completed bids may be submitted in online mode only as specified in Section-II of the NIT. Bids submitted through any other mode will not be accepted.
6. Bidders shall well acquaint themselves from tender wizard website and RECPDCL will not be responsible for any delay on account of website related issues on last date of bid submission. Submission a Late Bid Any delay, including postal delay, in the receipt of bid would be treated late submission of bid and shall be rejected.
7. Bids handed over at the Reception Counter or any other counter or room or to any person, other than the authorized person of RECPDCL, shall not be considered.
8. Language of Bids: The Bids prepared by the Bidder and documents relating to the bids exchanged by the Bidder and RECPDCL, shall be written in English language, provided that any printed literature furnished by the Bidder may be written in another language so long as the same is accompanied by an Hindi /English translation in which case, for purposes of interpretation of the bid, the English version shall govern.
9. **Bid Prices**
    - **a)** The prices shall be quoted in Indian Rupees only.
    - **b)** All taxes, duties, levies applicable etc. shall be clearly indicated.
    - **c)** Prices quoted must be final and shall remain constant throughout the period of validity of bid and shall not be subject to any upward modifications, whatsoever.
    - **d)** Bidders shall indicate their rates in clear/visible figures as well as in words and shall not alter/overwrite/make cutting in the quotation.
    - **e)** Conditional Financial Proposals will be rejected out rightly. Please note that the non-understanding of the scope of work at any stage will

not be construed as a reason for enhancement of fee/ price at a later stage.

10. **Bid Evaluation**

a) Bidder's details shall be evaluated with reference to the required documents submission criteria as mentioned in this tender document and subsequently on meeting the requirement, bids of bidders shall be considered for final/price evaluation.

b) The price bids shall be evaluated as under:

i. If there is any discrepancy between words and figures, the amount in words will prevail.

ii. ii. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and total price shall be corrected.

iii. If the Bidder does not accept the correction of the errors as above, the bid shall be rejected.

iv. The bidder whose evaluated price is found to be lowest (L-1), shall be considered for award of contract for Conducting Security Audit.

11. Payment Terms:

a) Payment will be released after successful completion of work, submission of necessary certificate /documents / Report to RECPDCL and receipt of pre-receipted bills in triplicate.

b) No advance payment shall be made.

c) No claim on account of any price variation / escalation shall be entertained.

d) No claim for interest in case of delayed payment will be entertained by RECPDCL

12. RECPDCL reserves the right to accept or reject any Bid, and to annul the Bidding process and reject all Bids at any time prior to Award of Contract without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds.

13. Force Majeure

a) "Force Majeure" means an event beyond the control of the Auditor and not involving the Auditor's fault or negligence and not foreseeable. This type of event may include but not limited to fires, explosions, floods, earthquakes, Pandemic, strikes, wars or revolutions etc.

b) The work execution period may be extended in case of Force Majeure condition. In order to be able to obtain an extension to the contract work period, the Auditor shall promptly notify auditee advising the existence of such an event, not later than one week of such event happening and produce the necessary documents such as Certificate of Chamber of

Commerce or any other competent authority indicating the scope of such an event, and its impact on the performance of the contract and establish that such an event is not attributable to any failures on its part.

14. Laws governing contract - The contract shall be governed by the laws of India for time being in force.
15. Jurisdiction of courts: The courts of Delhi shall alone have the jurisdiction to decide any dispute arising out of or in respect of the contract.
16. Arbitration: In the event of any dispute arising out of this notice inviting tender or any agreement arising the refrom or any matter connected or concerned with the said agreement in any manner of its implementation or any terms and conditions of the said agreement, the matter shall be referred to CEO-RECPDCL, who may himself act as sole arbitrator or may nominate an officer of RECPDCL as sole arbitrator, notwithstanding the fact that such officer has been directly or indirectly associated with the agreement. The bidder/ auditor will not be entitled to raise any objection for the appointment of such officer of RECPDCL as the sole arbitrator. The award of the arbitrator shall be final and binding subject to the provisions of the arbitration and conciliation Act, 1996 and rules made there under. The seat of arbitration shall be New Delhi and the language of arbitration shall be in English only.
17. The price bids of those firms will be opened who fulfils the terms and conditions.
18. Only those Organizations/firms registered with the CERT-in-empanelled for information security audit having valid CERT-In empanelment certificate on the date of tender publication are only eligible for submitting the quotation.
19. Incomplete or conditional quotation will not be entertained.
20. No quotation will be accepted after closing date and time.
21. Agencies to which work is awarded are not allowed to Sub-contract the work to any other parties either in part or full.
22. The agency will be removed from empanelment if due to any reason CERT-In has removed or not extended the empanelment of the agency.
23. The selected agency will not outsource any activity to other agency.
24. 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.
25. The selected agency shall submit the Model Non-Disclosure Agreement in the format as prescribed in Form VII in two (2) originals. The selected agency shall submit the Model Non-Disclosure Agreement on non-judicial stamp paper of Rs. 100/- each duly purchased from the National Capital Territory of Delhi.
26. Time Schedule: The first round of website 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.
27. The bidder may remain present himself /herself or his/her authorized

representative at the time of opening the quotation.

28. Any firm/organization blacklisted by a Govt./Semi Govt. Deptt. shall not be considered for this bid and bid will be rejected straightway.
29. 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.
30. The agency must have fully operational office/ Head office /Branch office in Delhi/NCR.
31. The Tender Committee reserves the right to relax any terms and condition in the Govt. interest, with the approval of competent authority.
32. All disputes are subject to the jurisdiction of the Courts in the N.C.T. of Delhi.
33. Prices should be indicated in Indian Rupees only and in the respective units indicated at each row.
34. 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.
35. 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.
36. The bidder shall be the single point of contact for RECPDCL till the completion of audit process & issuance of certificate.
37. 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.

38. Deliverables and Audit Reports:
    a) The successful bidder will be required to submit the following documents in printed format (2 copies each) after the audit of above-mentioned web & mobile application:
        i. A detailed report with security status and discovered vulnerabilities weakness and misconfigurations with associated risk levels and recommended actions for risk mitigations.
        ii. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by RECPDCL.

iii. The final security audit certificate for and should be in compliance with the NIC/MeitY/CERT-In standards, as applicable.

iv. All deliverables shall be in English language and in A4 size format.

v. The vendor will be required to submit the deliverables as per terms and conditions of this document.

vi. Server(s) required for carrying out the audit of the URJAMITRA Web Application including Web Services and Mobile application shall be in the scope of the bidder. The bidder shall be responsible for arranging the Server (s) from for the entire duration of the contract, till issuance of the security clearance certificate.

vii. The configuration of the production server of Urja Mitra application is: 1 VM (Application and database), 16vCPU, 64GB RAM, 500 GB Database and 50 GB Application (approx.), Linux (RHEL). The test Server(s) required for carrying out the audit of the URJAMITRA Web Application including Web Services and Mobile application shall be arranged with adequate configuration by the bidder.

viii. The Urja Mitra application has 32 modules (approx.), 165 nos (approx.) dynamic pages, 177 nos (approx.) static pages and 53 nos (approx.) Web Service/API included in the existing web application & 40 nos (approx.) screens each for Android & iOS mobile application which has to be audited under the present scope of work.

ix. The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.

x. The agency should provide support to the development team for changes in coding to remove the vulnerabilities.

xi. Vulnerability Assessment Report, Penetration Test Report.

xii. Compliance review should be done after ensuring that changes to remove the vulnerabilities are completed by the development team.

xiii. Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application or website or mobile application has no vulnerabilities as a result of changes done in the code

xiv. 1 day training session on the security for – No. of participants to also cover facilitation for closure of audit findings.

FORM-I

Letter for Submission of Financial Bid

(To be submitted on Company's letterhead duly signed)

To,

Addl. Chief Executive Officer
REC Power Development and Consultancy Ltd.
D Block REC World Head Quarter, Plot
No. I-4, Sector-29, Gurugram, Haryana-
122001

Sub.: To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application

Sir,

1. With reference to your Tender No. ---------- dated ---------- **To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application**

2. I wish to apply for engagement with RECPDCL

Further, I hereby certify that

a) I have read the provisions of the all clauses and confirm that notwithstanding anything stated elsewhere to the contrary, the stipulation of all clauses of Tender are acceptable to me and I have not taken any deviation to any clause.
b) I further confirm that any deviation to any clause of Tender found anywhere in my Bid, shall stand unconditionally withdrawn, without any cost implication whatsoever to the REC PDCL.
c) Our bid shall remain valid for period of 90 days from the last date of bid submission.

Date: **Signature: .....**

Place: **Full Name: .....**

Designation: .....

Address: .....

Note: In absence of above declaration/ certification, the Bid is liable to be rejected and shall not be taken into account for evaluation.

Form-II

BIDDER'S GENERAL DETAILS
(To be submitted on Company's letterhead duly signed)

To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application

GENERAL DETAILS

NIT NO……

1. **THE FIRM** _____
2. **Name** _____
3. **Regd.**

a)Address of Office:_____

_____

b) Contact Person's

i. Name & Design.:

ii. Address : _____

_____

iii. Tel No. Landline Mobile: _____

iv. Email ID: _____ _____

4. **Type of Firm (Please tick):** Private Ltd./Public Ltd./Cooperative/ Partnership/ Proprietor

5. PAN No.:_____ _____

6. GST Reg. No.:_____ _____

Signature……..……

Full Name……..

Designation……

Address……

Form-III

LETTER OF TRANSMITTAL

To,

Addl. Chief Executive Officer
REC Power Development and Consultancy Ltd.
D Block REC World Head Quarter,
Plot No. I-4, Sector-29,Gurugram, Haryana-
122001

Dear Sir/s,

I/We, the undersigned, have examined the details given in your Notice inviting Limited tender dated [**Insert Date**] FOR **To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application**

We accept all the terms & conditions of the bid document without any deviation and submit the Bid. We hereby certify that M/s _____ or its group companies have not been awarded any work for & shall not be a competitor to RECPDCL during contract period in case the contract is awarded.

Also, M/s _____or its group companies is not executing or providing any type of consultancy services either directly or as a sub-contractor for the particular work for which Bid is submitted.

It is confirmed that M/s. _____is not banned or blacklisted by any Govt./Pvt. Institutions in India.

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

FORM-IV

UNDERTAKING TOWARDS NOT BEING BLACK-LISTED
(On Company letter head)

I, _____ Authorized Signatory of M/s _____ hereby give undertaking that we, as a company are not black-listed by any Central/ State Government/ Semi-Government Organization/ Public Sector Undertaking/ Private Institution in India.

Further, if information furnished above stands false at any stage, we shall be completely liable for actions taken by RECPDCL as per terms & conditions of the tender including disqualification and exclusion from future contracts/assignments etc.

(Signature of Authorized Signatory)

Name*:

Designation*:

Seal:

FORM-V

FINANCIAL BID Format
(To be submitted in online mode only)

To engage CERT-IN empanelled security auditing agency to conduct security audit of URJAMITRA web application including web services and mobile application

Financial Bid:-

Name of the Bidder:

S. No.	Description	Amount (in Rs.)	GST Taxes (if any)	Total Price (in Rs.) (inclusive of all taxes including
1	Lump sum amount to Complete all levels of Security Audit of URJAMITRA Web Application including Web Services & Mobile Application in Android and IOS platform with Report Generation, recommendations and issue a Security Clearance Certificate. (As per scope of work, arrangement of test server & deliverables)			
GRAND TOTAL				
RUPEES IN WORDS				

Terms & Conditions:

1. In case of discrepancy between value indicated by the Bidder **"**In Figure**"** and **"**In words **"** at S**.**No**.** 3above, the value indicated at **"**In words**"** shall prevail**.**
2. Bidders have to quote as per financial bid format as above including all taxes & duties and GST. Financial bids will be evaluated based on total price quoted. At the

time of release of payment to the bidder, TDS /Labour cess will be deducted as the case may be.

3. If it is found that the tax quoted is higher than the applicable tax, in that case applicable taxes will only be paid by RECPDCL and if the tax quoted is lower than the applicable tax, in that case only the quoted taxes will be paid by the RECPDCL.

4. Rate quoted by the bidder shall remain firm & fixed and shall be binding on the Successful Bidder till completion of work.

5. The offer must be kept valid for a period of 90 days from the last date of bid submission. No escalation clause would be accepted. The validity can be further extended with mutual consent.

6. It will be the sole responsibility of the bidders to get the assessment of web services other parameters involved & its consideration before quoting the rates.

FORM-VI

Earnest Money Deposit Declaration

(To be submitted on bidder's letterhead)

Whereas, I/we (name of agency)……have submitted bids for ……(name of Goods /Work/Service) for tender no……dated …….

I/we hereby submit following declaration in lieu of submitting Earnest Money Deposit.

1. If after the opening of tender. I/we withdraw and/or modify my/our bid during the period of validity of tender (including extended validity of tender) as specified in tender documents.
2. If, after the award of work. I/we fail to sign the contract or to submit the performance guarantee before the deadline defined in the tender documents.

   I/we shall be suspended for one year and shall not be eligible to bid for REC Power Development and Consultancy Limited tenders from date of issue of suspension order.

Date: Signature with Seal of bidder(s)

Place: Full Company Address with Contact Details

FORM-VII

MODEL NON-DISCLOSURE AGREEMENT

(Between CERT-In empanelled Auditor & Auditee)

THIS NON-DISCLOSURE AGREEMENT is made on this …….. day (date) of …… (Year)

By and between

 # In case of Central Government Ministry/ Departments #/State Government Departments

President of India/Governor of (name of state) acting through…… (Name, Designation) of …….. (Name of Ministry/ Department) address …… hereinafter referred to as "Auditee" which expression shall unless repugnant to the context or meaning thereof, include its successors and assigns)of the first part.

 # In case of Autonomous Societies/ Not-for-profit companies/ Public sector Undertakings/Private sector

…… (Name of Company/ Society) incorporated /registered under the Companies Act, 1956/2013/ the societies registration Act, 1860 having its registered/corporate office at …… (hereinafter referred to as "Auditee" which expression shall unless repugnant to the context or meaning thereof, includes its successors, administrators and permitted assigns) of the first part.

And

Name incorporated/registered under the……..Name of the Act having its registered/ corporate office at …… (herein referred to as "Auditor" which expression shall unless repugnant to the context or meaning thereof, includes its seccessors, assigns, administrators, liquidators and recievers)of the second part

WHEREAS

A. Auditor is a services organization empanelled by the Indian Computer Emergency Response Team (hereinafter CERT-IN) under Department of Electronics & IT, for auditing, including vulnerability assessment and penetration testing of computer systems, networks, computer resources & applications of various agencies or

departments of the Government, critical infrastructure organizations and those in other sectors of Indian economy vide communication No……dated…….

B. Auditor as an empanelled Information Security Auditing organization has agreed to fully comply the "Guidelines for CERT-In Empanelled Information Security Auditing Organizations, Terms & conditions of empanelment and Policy guidelines for handling audit related data" while conducting audits.

C. Auditee is also aware of the aforesaid Guidelines along with guidelines for Auditee Organizations published by CERT-In.

D. Both Auditor and Auditee have given their irrevocable consent to fully comply the aforesaid Guidelines and any amendments thereof without any reservations.

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. **Definitions.** :

(a) The term "Confidential Information" shall include, without limitation, all information and materials, furnished by either Party to the other in connection with Auditee products and services including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic media, and including all proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, business or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to Auditee products and services. Results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. shall also be considered Confidential Information.

(b) The term "Auditee products" shall include all such products, goods, services, deliverables, which are subject to audit by the empanelled auditor under the Agreement.

2. **Protection of Confidential Information.** With respect to any Confidential Information disclosed to it or to which it has access, Auditor affirms that it shall:

(a) Use the Confidential Information as necessary only in connection with scope of audit and in accordance with the terms and conditions contained herein;

(b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its other clients;

(c) Not to make or retain copy of any details of products and/or services, prototypes, business or marketing plans, Client lists, Proposals developed by or originating from Auditee or any of the prospective clients of Auditee.

(d) Not to make or retain copy of any details of results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. without the express written consent of Auditee.

(e) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of theauditee ; and

(f) Return to theauditee, or destroy, at auditee's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately on (i) expiration or termination ofthis agreement, or (ii) the request of Auditee therefor.

(g) Not to send Auditee's audit information or data and/or any such Confidential Information at any time outside India for the purpose of storage, processing, analysis or handling without the express written consent of the Auditee.

(h) The auditor shall use only the best possible secure methodology to avoid confidentiality breach, while handling audit related data for the purpose of storage, processing, transit or analysis including sharing of information with auditee.

(i) Not to engage or appoint any non-resident/foreigner to undertake any activity related to Information Security Audit. In case of information security audits for Government/ critical sector organization, only the man power declared to CERT-In shall be deployed to carry out such audit related activities.

(j) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the Auditor and the Auditee or the nature of services to be provided by Auditor to the Auditee.

(k) Make sure that all the employees and/or consultants engaged to undertake any audit on its behalf have signed the mandatory non-disclosure agreement.

3. **Onus.** Auditor shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.

4. Permitted disclosure of audit related information:

The auditor may share audit information with CERT-In or similar Government entities mandated under the law as and when called upon to do so by such agencies with prior written information to the auditee.

5. **Exceptions.** The Confidentiality obligations as enumerated in Article 2of this Agreement shall not applyin following cases:

(a) Which is independently developed by Auditor or lawfully received from another source free of restriction and without breach of this Agreement; or

(b) After it has become generally available to the public without breach of this Agreement by Auditor; or

(c) Which at the time of disclosure to Auditor was known to such party free of restriction and evidenced by documents in the possession of such party; or

(d) Which Auditee agrees in writing is free of such restrictions.

(e) Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;

6. **Remedies**. Auditor acknowledges that any actual or threatened disclosure or

use of the Confidential Information by Auditor would be a breach of this agreement and may cause immediate and irreparable harm to Auditee or to its clients; Auditor affirms that damages from such disclosure or use by it may be impossible to measure accurately; and injury sustained by Auditee / its clients may be impossible to calculate and compensate fully. Therefore, Auditor acknowledges that in the event of such a breach, Auditee shall be entitled to specific performance by Auditor of its obligations contained in this Agreement. In addition Auditor shall compensate the Auditee for the loss or damages caused to the auditee actual and liquidated damages which may be demanded by Auditee. Liquidated damages not to exceed the Contract value. Moreover, Auditee shall be entitled to recover all costs of litigation including reasonable attorneys' fees which it or they may incur in connection with defending its interests and enforcement of contractual rights arising due to a breach of this agreement by Auditor. All rights and remedies hereunder are cumulative and in addition to any other rights or remedies under any applicable law, at equity, or under this Agreement, subject only to any limitations stated herein.

7. **Need to Know**. Auditor shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees and/or consultants of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the Auditee. No information relating to auditee shall be hosted or taken outside the country in any circumstances.

8. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

9. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

10. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations

hereunder.

11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the jurisdiction of Courts and/or Forums situated at < Name of the city>

12. **Entire Agreement**. This Agreement constitutes the entire understanding and agreement between the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

15. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

16. **Waiver.** Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be waiver of any preceding or succeeding breach of the same or any other provision hereof.

17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after expiration or termination of this Agreement.

18. **Non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years Auditor shall not solicit or attempt to solicit Auditee's

employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct business similar to Auditee with any employee and/or consultant of the Auditee who has knowledge of the Confidential Information, without the prior written consent of Auditee.

19. This Agreement is governed by and shall be construed in accordance with the laws of India. In the event of dispute arises between the parties in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, the parties shall attempt to resolve the dispute in good faith by senior level negotiations. In case, any such difference or dispute is not amicably resolved within forty five (45) days of such referral for negotiations, it shall be resolved through arbitration process, wherein both the parties will appoint one arbitrator each and the third one will be appointed by the two arbitrators in accordance with the Arbitration and Conciliation Act, 1996. The venue of arbitration in India shall be (please choose the venue of dispute resolution as the city) or where the services are provided. The proceedings of arbitration shall be conducted in English language and the arbitration award shall be substantiated in writing and binding on the parties. The arbitration proceedings shall be completed within a period of one hundred and eighty (180) days from the date of reference of the dispute to arbitration.

20. **Term.** This Agreement shall come into force on the date of its signing by both the parties and shall be valid up to …… year.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

 # In case of auditee being Central Government Ministry/ Departments #

For & on behalf of President of India
(Name and designation of authorized signatory)
……
<Name of Central Govt. Ministry/Department>

Or

 # In case of auditee being State Government Department #

For & on behalf of Governor of ……. < State name>

……..

(Name and designation of authorized signatory)

<Name of State Department>

Or

 # In case of Autonomous Societies/Not-for-profit-company/Public sector undertaking /Private Sector #

for <Name of organization> , <Name and designation of authorized signatory> duly authorized by rules & regulations / of <Name of society>/ vide resolution no. …. Dated ……. Of Board of Directors of .....<Name of organization>.

(AUDITEE) **(AUDITOR)**

WITNESSES:

1.

2.

FORM-VIII

EMPANELLED INFORMATION SECURITY AUDITING ORGANISATIONS by CERT-In

The List of IT Security Auditing Organizations, as given below, is up-to-date valid list of CERT-In Empanelled Information Security Auditing Organizations. This list is updated by us as soon as there is any change in it.

1. M/s AAA Technologies Ltd

278-280, F-Wing, Solaris-1,
Saki Vihar Road, Opp. L&T Gate No. 6,
Powai, Andheri (East),
Mumbai – 400072.
Website URL: http://www.aaatechnologies.co.in
Ph: 022-28573815 / 16
Fax: 022-40152501
Contact Person: Mr. Anjay Agarwal, Chairman & Managing Director
Mobile: +91 09322265876, 9821087283
E-mail: anjay[at]aaatechnologies.co.in

2. M/s AKS Information Technology Services Pvt Ltd

B-21, Sector-59, Noida - 201309 (Uttar Pradesh)
Website URL: https://www.aksitservices.co.in/
Ph: 0120-4545911
TeleFax : 0120-4243669
Contact Person: Mr. Ashish Kumar Saxena, Managing Director
Mobile: +91-7290058951
E-mail: info.cert[at]aksitservices.co.in

3. M/s AQM Technologies Pvt Ltd.

A 401, Raheja Plaza, LBS Road, Nityanand Nagar, Ghatkopar West,
Mumbai, Maharashtra 400086, INDIA
Phone number: 022 4050 8200
Contact Person: Mr. Sanjay PARIKH
E-mail:sanjay.parikh[at]aqmtechnologies.com
Contact No: +91-8291858027 / 022-40508262

4. M/s Allied Boston Consultants India Pvt. Ltd.

2205, Express Trade Towers-2, B-36, Sector 132,
Noida Expressway, Noida 201301 (U.P.)
Ph: 9891555625, 0120-4113529
Fax: 0120-4113528
Contact Person: Mr. T. Ganguly
E-mail: itsec[at]alliedboston.com

5. M/s A3S Tech & Company

A/95, Kamla Nagar, Delhi-110007
Ph: 9810899624
Fax: 23933429
Contact Person: Sagar Gupta
E-mail: sagar[at]a3stech.co.in

6. M/s Andhra Pradesh Technology Services Ltd
(Govt. of AP Undertaking)

3rd Floor, R&B Building, MG Road, Labbipet,
Vijayawada, Andhra Pradesh 520010
URL: https://www.apts.gov.in/
Land line Phone: 08662468105;
Mobile phone: 9440469194
Contact Person: Dr. G Jacob Victor, Executive Director
E-mail: mgr-apcsp-apts[at]ap[dot]gov[dot]in
Alternate Email ID: VictorJacob[dot]G[at]gov[dot]in

7. M/s ANB Solutions Private Limited

901, Kamla Executive Park, Off Andheri-Kurla Road,
J. B. Nagar, Andheri East, Mumbai 400 059
Ph: +91 (22) 4221 5300
Fax: +91 (22) 4221 5303
Contact Person: Preeti Raut
E-mail:preeti.kothari[at]anbglobal.com

8. M/s AGC Networks Limited

Essar House, 11, K. K. Marg, Mahalaxmi,
Mumbai-400034, Maharashtra, India
Ph: +91-9930134826, Landline: +91 022 66601100
Contact Person: Mr. Anant N. Bhat
E-mail: anant.bhat[at]agcnetworks.com

9. M/s Accenture Solutions Pvt. Ltd.

Accenture BDC7C, Piritech Park (SEZ), Phase 1,
RMZ Ecospace Internal Rd, Adarsh Palm Retreat, Bellandur,
Bengaluru, Karnataka 560047, India
Ph: 9916011888
Contact Person: Prasanna Ramasamy
E-mail: Prasanna.ramasamy[at]accenture.com

10. M/s Amigosec Consulting Private Limited

401, Shatrunjay, Divecha Complex, Edulji Road, Charai,
Thane(w), Maharashtra - 400601
Ph : +91 9819080470
Contact Person: Mr. Ashish Rao
E-mail: ashish.p.rao[at]synradar.com

11. M/s ANZEN TECHNOLOGIES PVT. LTD.

A-429, Second Floor, A-Wing, Vashi Plaza, Sector 17,
Vashi, Navi Mumbai, 400703
Ph: 09821775814
Contact Person: Ramesh Tendulkar
E-mail :rtendulkar[at]anzentech.com

12. M/s Attra Infotech Pvt. Ltd

No. 23 & 24, 2nd Floor, AMR Tech Park II,
Hongasandra, Bengaluru – 560068
Ph: 91 80 4197 0900
Contact Person:

• Riaz Kakroo - Global Head – Corporate Infosec
riaz.kakroo[at]attra.com.au / 9686579832
• Santosh Lohani – Head of practice (cybersecurity)
Santosh.lohani[at]attra.com.au/ 9741399220

13. M/s Aujas Cybersecurity Limited

#595, 4th Floor, 15th Cross, 24th Main Rd, 1st Phase,
J. P. Nagar, Bengaluru, Karnataka 560078
Ph: +91 9980238005
Contact Person: Jaykishan Nirmal
E-mail: Jaykishan.Nirmal[at]aujas.com

14. M/s AURISEG CONSULTING PRIVATE LIMITED

NO 666/81, MAVEERAN DURAISWAMY STREET,
POONGA NAGAR, THIRUVALLUR
Ph: +91 99408 64275
Landline Phone Number: +91 44 42017437
Contact Person: M.S SRINIVASAN - DIRECTOR -CONSULTING PRACTICE
E-mail: SRINI.MANI [at] AURISEG.COM

15. M/s BHARAT ELECTRONICS LIMITED

Office of the GM/Software,
BEL Software SBU
Bharat Electronics Limited
Jalahalli, Bengaluru - 560013
Karnataka
Ph: 080-22197197, or 080-28383120
Fax: 080-28380100
Contact Person: Mr. Ramesh Prabuu V, DGM (Software Marketing), BEL/SW
E-mail: ITSecurityAuditTeam[at]bel.co.in
Mobile: +91 9945193542
Ph : 080-22195714

16. M/s Bharti Airtel Service Limited

Plot# 16, Udyog Vihar-Phase-IV
Sector 18, Gurgaon-122016
Ph: +91-9987891999
Contact Person: Amit Chaudhary
E-mail: amit.chaudhary[at]airtel[dot]com

17. M/s BDO India LLP

The Ruby, Level 9, North West Wing, 29, Senapati Bapat Marg,
Dadar West, Mumbai, 400028.
Ph: +91 022 62771600
Fax: +91 022 62771600
Contact Person: Mr. Mubin Shaikh / Mr. Nipun Jaswal
E-mail: mubinshaikh[at]bdo.in / nipunjaswal[at]bdo.in

18. M/s Centre for Development of Advanced Computing (C - DAC)

Plot No. 6 & 7, Hardware Park,
Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510
Ph: +919441233972, +917382303598
Contact Person: Ch A S Murty
E-mail: cswan[at]cdac.in, chasmurty[at]cdac.in

19. M/s Crossbow Labs LLP

Unit 406, Brigade IRV Center, Nallurhalli,
Whitefield, Bangalore
Karnataka 560066,
India
Ph : +91 80 470 91427
Contact Person: Mr. Rosan Thomas
E-mail: cert[at]crossbowlabs.com

20. M/s CyberQ Consulting Pvt Ltd.

J-1917, Chittaranjan Park, New Delhi - 110019
Ph: 7982895613/7042081393
Contact Person: Mr. Debopriyo Kar / Mr. Rajiv Malhotra
E-mail:debopriyo.kar[at]cyberqindia.com
shikha.yadav[at]cyberqindia.com
ankita.chatterjee[at]cyberqindia.com

21. M/s CyRAAC Services Private Limited

2nd Floor, Napa Prime, 7/24, 11th Main Road,
4th Block East, Jayanagar,
Bengaluru - 560011
Ph.: +919886210050
Contact Person: Mr. Murari Shanker
E-mail: ms[at]cyraacs.com

22. M/s Codec Networks Pvt Ltd

B-136, Surajmal Vihar, Delhi 110092
Ph: +91 9971676124, +91 9911738718
Contact Person: Mr. Piyush Mittal
E-mail: amittal[at]codecnetworks[dot]com; piyush[at]codecnetworks[dot]com

23. M/s Cyber Security Works Pvt. Ltd.

No.6, 3rd Floor, A-Block, IITM Research Park
Taramani, Chennai – 600 113
Ph : +91-44-42089337
Contact Person: Mr. Ram Swaroop M
E-mail: ram[at]cybersecurityworks.com

24. M/s CEREIV Advisory LLP

Chembakam Building, Koratty Infopark, Thrissur Dt, Kerala - 680 308
Ph : 9745767949
Contact Person: Mridul Menon
E-mail: mridul[at]cereiv.com

25. M/s ControlCase International Pvt. Ltd.

Corporate Center, Level 3, Andheri-Kurla Road, Marol,
Andheri (East), Mumbai 400059, Maharashtra.
Ph :+91 22 6647 1800
Fax: +91 22 6647 1810
Contact Person : Mr. Satya Rane
E-mail : certinaudit[at]controlcase.com

26. M/s CyberSRC Consultancy LLP

Unit no 605, 6th floor, World Trade Tower,
Sector 16 Noida - Uttar Pradesh 201301
Ph :+91 8800377255, +91 120 4160448
Contact Person : Vikram Taneja, CEO
E-mail :vikram[at]cybersrcc.com , info[at]cybersrcc.com

27. M/s Dr CBS Cyber Security Services LLP

113, Suraj Nagar East, Civil Lines, Jaipur, Rajasthan-302006
Ph : 0141-2229475, +91- 9414035622, 9828877777
Contact Person: Dr C B Sharma IPS Retd.
E-mail: contact[at]drcbscyber.com, drcbscyber[at]gmail.com

28. M/s Deloitte Touche Tohmatsu India LLP

7th Floor, Building 10, Tower B, DLF Cyber City Complex,
DLF City Phase II, Gurgaon, Haryana, India
Ph : +91 9811663776
Fax: 0124-6792012
Contact Person: Mr. Gautam Kapoor
E-mail: gkapoor[at]deloitte.com

29. M/s Deccan Infotech (P) Ltd.

13, Jakkasandra block. 7th cross.
Koramangala. Bengaluru - 560034
Ph : 080 - 2553 0819
Contact Person: Mr. Dilip Hariharan
E-mail: dilip[at]deccaninfotech.in

30. M/s eSec Forte Technologies Pvt. Ltd.

Postal address:311, Jwala Mill Road, Udyog Vihar - Phase 4,
Gurugram, Haryana, 122015, India
Ph : +91 9871699555
Fax: +91 0124 4264666
Contact Person: Kunal Bajaj
E-mail: kunal[at]esecforte.com

31. M/s Ernst & Young LLP

Golf View Corporate Tower B Sector - 42,
Sector Road
Ph: +91 124 4431380, +91 9650711300
Contact Person: Mr. Vidur Gupta
E-mail:Vidur.gupta[at]in.ey.com

32. M/s ESSENTIAL INFOSEC PRIVATE LIMITED

Corporate address (Mailing Address):
1st Floor, Plot No. 16, Near SBI BANK Behind Sultanpur Metro Station, New Delhi 110030

Registered Address:
Flat No. 304, Plot No. 2, Shivam Palace, Mamdapur-Neral, Tal. Karjat, Dist. Raigad, Raigarh MH 410101
Ph: 011 4065 6797
Mob: +91 79855 34793
Contact Person: Pawan Srivastav, Director
E-mail: cert[at]essentialinfosec.com

33. M/s FIS Global Business Solutions India Pvt. Ltd.

402, I Park, Plot No. 15, Phase IV, Gurugram, Haryana 122016
Ph.: +919811865050
Contact Person: Jatin Jain
E-mail: Jatin.Jain[at]fisglobal.com

34. M/s GRM Technologies Private Limited

Postal address: Corporate address:No-9, 2nd floor Shoba Homes, West Tambaram, Chennai600045,India.
Registered office address: 2/127,Mani Sethupattu, Sriperumbudur Taluk, Kancheepuram
District, Tamil Nadu-601 301, India.
Ph: +91-9042000525, +91-44-22261489, +91-94873 88551
Contact Person: Mr. Babu G / Mr. Ashok Kumar
E-mail: babug[at]grmtechnologies.com/ashok[at]grmtechnologies.com

35. 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. Akshay Garkel, Partner Cyber
Mobile: +91 9820208515
E-mail: Akshay.Garkel[at]IN.GT.COM and cyber[at]IN.GT.COM

36. M/s G.D.Apte & Co.

GDA House, Plot No. 85, Right Bhusari Colony,
Paud road, Pune 411038
Ph : 020 6680 7200
Fax: 020 2528 0275
Contact Person: Prakash P. Kulkarni
E-mail: prakash.kulkarni[at]gdaca.com

37. M/s HackIT Technology And Advisory Services

64/2453, 2nd Floor,
JVC Tower, Kaloor-Kadavanthara Road
Kaloor PO, Cochin, Kerala, India
PIN - 682 017
Ph: (+91) 484 4044 234
Contact Person: Akash Joseph Thomas
E-mail: akash[at]hackit.co

38. M/s Hewlett Packard Enterprise India Pvt Ltd.

#24, Salarpuria Arena, Hosur Main Road, Adugodi, Bangalore-560030, India
Ph : 9945611299
Contact Person: Malligarjunan Easwaran
E-mail: malligarjunan.e[at]hpe.com

39. M/s ITORIZIN TECHNOLOGY SOLUTIONS PVT LTD

8/14, SHAHID NAGAR, GROUND FLOOR. WING “A”.
KOLKATA – 700078. West Bengal, India
Ph : 9883019472
Contact Person: Sangeeta Ganguly
E-mail: g.sangeeta[at]itorizin[dot]in / connect[at]itorizin[dot]in

40. M/s Information Security Management Office (ISMO)

Department of Information Technology, Electronics & Communication, Haryana,
SCO 109-110, First Floor, Sector-17-B, Chandigarh – 160017
Ph : +91 7042824602, +91 9417362127
Contact Person: Sh. Sudipta Choudhury and Sh. Amit Kumar Beniwal
E-mail: sudipta.ditech[at]hry.gov.in, amit.beniwal[at]haryanaismo.gov.in

41. M/s Innovador Infotech Private Limited

1128, Ahmamau, Beside Lucknow Treat Restaurant,
Near Sultanpur Road Roundabout, Shaheed Path,
Arjunganj, Lucknow- 226002 (Uttar Pradesh)
Ph.: +91-8896605755
Contact Person: Rahul Mishra
E-mail: rahul[at]innovadorinfotech.com

42. M/s ISECURION Technology & Consulting PVT LTD

2nd floor, #670, 6th Main Road, RBI Layout, J.P. Nagar 7th Phase, opp. Elita Promenade,
Bengaluru, Karnataka 560078
Ph : 8861201570
Contact Person: Manjunath NG
E-mail: manjunath[at]isecurion.com

43. M/s KPMG Assurance and Consulting Services LLP

DLF Building No. 10, 8th Floor, Tower C,
DLF Cyber City, Phase 2,
Gurgaon, Haryana-122002
Ph : +91 9810081050
Fax: +91 124 254 9101
Contact Person: Mr. Atul Gupta (Partner, Cyber Security)
E-mail: atulgupta[at]kpmg.com

44. M/s Kochar Consultants Private Limited

302, Swapnabhoomi A Wing,
S.K. Bole Road, Nr Portuguese Church,
Dadar (W), Mumbai 400028.
Ph : 24229490 / 24379537 / 9819846198 / 9869402694
Fax: 24378212
Contact Person: Mr. Pranay Kochar
E-mail: pranay[at]kocharconsultants.com

45. M/s KRATIKAL TECH PRIVATE LIMITED

A-130, SECOND FLOOR, SECTOR 63, NOIDA - 201301
Ph : 7042292081, 9651506036
Contact Person: PAVAN KUMAR
E-mail: PAVAN[at]KRATIKAL.COM

46. M/s MapleCloud Technologies

B4/102-C, Keshavpuram, Delhi - 110035
Ph : +91-9739995151 / +91-8178803636
Contact Person: Yogendra Rajput
E-mail: yogendra.rajput[at]maplecloudtechnologies.com
: yogendra.rajput[at]mcts.in

47. M/s MOBITRAIL

Office No 205, Triumph Estate, Near Express Zone, Goregaon East, Mumbai 400063
Phone No: +91 9867386146
Fax: 022-28782751

Contact Person: Vikas Kedia
E-mail: Vikas@MobiTrail.com

48. M/s Mahindra Special Services Group

(Division of Mahindra Defence Systems Limited)
Mahindra Towers, P.K Kurne Chowk,
Dr. G.M Bhosale Marg, Worli,
Mumbai - 400018, India
Ph: 9769015546
Contact Person: Mr. Rajesh Huddar
E-mail :rajesh.huddar[at]mahindrassg.com

49. M/s Maverick Quality Advisory Services Private Limited

123 RADHEY SHYAM PARK P.O SAHIBABAD
Ghaziabad, U.P, INDIA – 201005
Ph :9871991928
Contact Person : Mr. Ashok Vardhan,Director
E-mail :ashok[at]mqasglobal.com

50. Madhya Pradesh Agency for Promotion of Information Technology (MAP_IT) (A Regt. Society of Department of Science & Technology, Govt of Madhya Pradesh)

47-A , State IT Center, Arera Hills,
Bhopal, Madhya Pradesh- 462011
Ph: 0755-2518713, 0755-2518702
Fax: 0755-2579824
Contact person : Mr. Vinay Pandey
Mobile:+91-0755-2518710
Email: vinay[dot]pandey[at]mapit [dot] gov [dot] in

51. M/s Mirox Cyber Security & Technology Pvt Ltd

4th Floor Nila Technopark Kariyavttom PO 695581
Trivandrum, Kerala
Phone +91 471 4016888 / +91 471 4000545
Mobile 9995199499, 9995799499

Contact Person : Mr. Rajesh Babu
Mobile: 9995799499
Email- rb[at]miroxindia.com/rbmirox2000[at]gmail.com

52. M/s Net Square Solutions Private Limited

1, SanjivBaug baug, Near Parimal Crossing, Paldi,
Ahmedabad - 380007, Gujarat
Fax : +91 7926651051
Contact Person : Ms. Pradnya Karad
Email: pradnya[at]net-square.com
Mobile: +91 7767955575

53. M/s Network Intelligence India Pvt. Ltd.

2nd Floor, 204, Ecospace IT Park,
Off Old Nagardas Road, Andheri-E, Mumbai-400069.
Ph :+919820049549
Contact Person : Mr. Kanwal Kumar Mookhey
E-mail :kkmookhey[at]niiconsulting.com

54. M/s Nangia & Co LLP

A-109, Sector 136, Noida (Delhi-NCR) - 201304
Ph : +91 98203 65305
Fax: +91 120 259 8010
Contact Person : Shrikrishna Dikshit
E-mail : shrikrishna.dikshit[at]nangia.com, poonam.kaura[at]nangia.com

55. M/s Netmagic IT Services Pvt. Ltd.

Lighthall 'C' Wing, Hiranandani Business Park, Saki Vihar Road,
Chandivali, Andheri (East) Mumbai 400 072
Ph :02240099099
Fax:02240099101
Contact Person : Mr. Yadavendra Awasthi
E-mail : yadu[at]netmagicsolutions.com

56. M/s Netrika Consulting India Pvt. Ltd.

Plot no.2, Industrial Estate, Udyog Vihar, Phase-IV,
Gurugram, Haryana, India. PIN: 122015
Ph : +91-124-4883000
Contact Person : Sanjay Kaushik & Rajesh Kumar
E-mail : sanjay[at]netrika.com; rajesh.kumar[at]netrika.com

57. M/s Netsentries Infosec Solutions Private Limited

No.5, 4th Floor, Wing II
Jyothirmaya Building, Infopark SEZ Phase-II,
Brahmapuram P.O. Cochin 682303
Ph :+91 8884909578
Contact Person : Sudheer Elayadath
E-mail : Sudheer[at]netsentries.com

58. M/s NG TECHASSURANCE PRIVATE LIMITED

Shop No. F-07 (107), First Floor, Atlanta Shopping Mall,
Althan Bhimrad Road, Surat, Gujarat - 395017
Ph : +91 98989-51269
Contact Person : Mr. Gaurav Goyal
E-mail : admin[at]ngtech.co.in

59. M/s Lucideus Technologies Pvt. Ltd

A-1/20, Basement, Safdarjung Enclave, New Delhi- 110029
Ph : +91 9717083090
Contact Person : Hitesh Butani
E-mail : hitesh.b@lucideustech.com

60. M/s Oxygen Consulting Services Private Limited

COSMOS, E/701, Magarpatta City, Hadapsar, Pune 411028
Ph :+91 9890302009, +91 9370288368, +91 02048620461
Contact Person : Mr. Sanjiv Agarwala
E-mail : sanjiv.agarwala[at]o2csv.com
ska262001[at]yahoo.co.in

61. M/s Panacea InfoSec Pvt. Ltd.

226, Pocket A2, Sector 17, Dwarka, New Delhi - 110075
Ph : +91 11 49403170
Primary Contact Person : Apurva K Malviya, Global Business Head
E-mail : apurva[at]panaceainfosec.com
Mobile: +91-9650028323/ +91 9205786094
Secondary Contact Person : Chandani Mishra, AVP IT Security
E-mail : cg[at]panaceainfosec.com
Mobile: +91-8929768061

62. M/s Peneto Labs Pvt Ltd

Level 8 & 9, Olympia Teknos, No - 28, SIDCO Industrial Estate, Guindy, Chennai 600032
Ph :+91 8861913615 / +91 44 4065 2770
Contact Person : Parthiban J
E-mail :Parthiban[at]penetolabs.com

63. M/s Paladion Networks Pvt. Ltd.

Shilpa Vidya, 49 1st Main, 3rd Phase
JP Nagar, Bangalore - 560078
Ph : +91-80-42543444
Fax: +91-80-41208929
Contact Person : Mr. Balaji Venkatasubramanian
E-mail : balaji.v[at]paladion.net

64. M/s Payatu Technologies Pvt Ltd

502,5th Floor, Tej House,
5 MG Road, Camp, Pune-411001
Ph : +91-20-41207726
Contact Person: Mr. Pranshu Jaiswal
E-mail: cert[at]payatu.com

65. M/s Price water house Coopers Pvt. Ltd.

7th & 8th Floor, Tower B, Building 8,
DLF Cyber City, Gurgaon, Haryana -122002

Ph : [91] 9811299662
Fax: [91] (124) 462 0620
Contact Person: Mr.Rahul Aggarwal
E-mail : rahul2.aggarwal[at]pwc.com

66. M/s Protiviti India Member Private Limited

GTB Nagar, Lalbaug, Everard Nagar,
Sion, Mumbai, Maharashtra 400022
Ph :022 6626 3333
Contact Person: Mr. Sandeep Gupta (Managing Director)
E-mail :Sandeep.Gupta[at]protivitiglobal.in
Phone: +91-9702730000

67. M/s PRIME INFOSERV LLP

60, SIBACHAL ROAD, BIRATI, KOLKATA 700051
Ph : 033- 40085677, Mobile no.- +91 9830017040
Contact Person: Sushobhan Mukherjee
E-mail: smukherjee[at]primeinfoserv[dot]com, info[at]primeinfoerv[dot]com

68. M/s Qseap Infotech Pvt. Ltd.

Unit No.105, Building No.03, Sector No.03,
Millennium Business Park, Mahape(MIDC),
Maharashtra- 400710, India
Ph :9987655544
Contact Person: Mr. Abhijit Doke
E-mail :certin[at]qseap.com

69. M/s QRC Assurance and Solutions Private Limited

Office No 508, Plot No 8, Ellora Fiesta, Sector -11,
Sanpada, Navi Mumbai, Maharashtra, India, 400705
Ph : +91-9920256566
Contact Person: Kalpesh Vyas
E-mail: kalpesh.vyas[at]qrcsolutionz[dot]com

70. M/s QA InfoTech Software Services Private Limited

A-8, Sector 68, Noida, Uttar Pradesh, 201309
Ph : +91-120-6101-805 / 806
Contact Person: Mr Rajesh Sharma (Co-Founder and Chief Information Officer)
E-mail: rajesh[at]qainfotech.com

71. M/s Risk Quotient Consultancy Private Limited

Unit 9, Building No:02, Sector 3, Plot No:1,
Millennium Business Park, Mahape, Navi Mumbai 400701
Ph :9821340198
Contact Person : Ms.Deepanjali Kunthe
E-mail :deepanjali.kunthe[at]rqsolutions.com

72. M/s RSM Astute Consulting Pvt. Ltd.

301-307, A Wing, Technopolis Knowledge Park,
Mahakali Caves Road, Andheri (East),
Mumbai – 400093
Tel: 91-22- 6108 5555
Contact Person: Mr. Anup Nair
E-mail: anup.nair[at]rsmindia.in
Mobile No. +91 8828428080
Website: www.rsmindia.in

73. M/s RNR Consulting Private Limited

E-16/169, Sector-8, Rohini, Delhi 110085
Ph : +91 9999132873 , +91 9971214199
Contact Person: Nitish Goyal , Practice Head – Information and Cyber Security
E-mail: nitish[at]consultrnr[dot]com

74. M/s SecureLayer7 Technologies Private Limited

Plot No. 28, Vyankatesh Nagar, Beside Totala Hospital,
Jalna Road, Aurangabad, MH 431001
Ph : +91-844-844-0533
Contact Person: Mr. Sandeep Kamble
E-mail: cert[at]securelayer7.net

75. M/s SecurEyes Techno Services Pvt. Ltd.

4th Floor, Delta Block, Sigma Soft Tech Park,
Whitefield Main Road, Varathur, Bangalore - 560066
Phone Number: +91 9449035102/ 080-41264078
Contact Person: Ms. Uma Pendyala
E-mail :umap[at]secureyes.net

76. M/s Security Brigade InfoSec Pvt. Ltd.

3rd Floor, Kohinoor Estate, Lower Parel,
Mumbai - 400013
Ph : +919004041456
Contact Person: Mr. Jamila Pittalwala
E-mail: certin[at]securitybrigade.com

77. M/s Sysman Computers

312, Sundram, Rani Laxmi Chowk,
Sion Circle, Mumbai 400022
Ph : 99672-48000 / 99672-47000 / 022-2407-3814
Website: www.sysman.in
Contact Person: Dr. Rakesh M Goyal, Director
E-mail: rakesh[at]sysman.in

78. STQC Directorate, Ministry of Electronics and IT, Govt. of India

Electronics Niketan, 6 C G O Complex, Lodhi Road, New Delhi-110003
Ph :011 24301816, 24301382
Fax:011 24363083
Contact Person: Mr. Gautam Prasad
E-mail: gprasad[at]stqc.gov.in; headits[at]stqc.gov.in

79. M/s Sattrix Information Security Pvt. Ltd.

28, Damubhai Colony, Nr. Anjali Cross Road, Bhatta,
Paldi, Ahmedabad-380007.
Ph : +91 9825077151
Contact Person: Bhavik Patel
E-mail: bhavik.patel[at]sattrix[dot]com

80. M/s Suma Soft Private Limited

Suma Center, 2nd Floor,
Opp. Himali Society, Erandawane,
Pune, Maharashtra – 411 004.
Tel: +91.20.4013 0700, +91.20.4013 0400
Fax: +91.20.2543 8108
Contact Person: Mr. Milind Dharmadhikari,
Practice Head - IT Risk & Security Management Services
E-mail:milind.dharmadhikari[at]sumasoft.net / infosec[at]sumasoft.net
Mobile - +91-98700 06480

81. M/s SISA Information Security Private Limited

No. 79, Road Number 9, KIADB IT PARK,
Arebinnamangala Village, Jala Hobli
Bengaluru, Karnataka, India - 562149
Ph : +91-7042027487
Contact Person: Mr. Bharat Malik
E-mail : warlabs[at]sisainfosec.com

82. M/s Sequretek IT Solutions Pvt. Ltd.

304, Satellite Silver, Andheri Kurla Road, Marol,
Andheri East, Mumbai, INDIA - 400 097
Ph : 022-40227034
Fax: 022-40227034
Contact Person: Anup Saha (anup.saha@sequretek.com)
E-mail: info[at]sequretek.com (Official)

83. M/s Siemens Limited

Birla Aurora Towers, Level 21, Plot 1080, Dr. Annie Basant Road,
Worli, Mumbai - 400030
Ph : +91 22 39677640
Contact Person: Amitava Mukherjee
E-mail:Amitava.Mukherjee[at]siemens.com

84. M/s Software Technology Parks Of India

1st Floor, Plate B, Office Block-1,
East Kidwai Nagar, New Delhi-110023
Website URL: http://www.stpi.in
Ph :+91-11-24628081
Fax:+91-11-20815076
Contact Person: Mr.Paritosh Dandriyal, Director
E-mail :paritosh[at]stpi[dot]in

85. M/s Sumeru Software Solutions Private Limited

1st Floor "Samvit", Near The Art of Living International Center,
21st KM Kanakapura Main Road,
Udayapura, Bangalore – 560082
Karnataka, India
Ph : +91 6364357139
Fax: +91 80-4121 1434
Contact Person: Asish Kumar Behera
E-mail: cert-in[at]sumerusolutions.com

86. M/s SWADESH SYSTEM PVT.LTD.

504,5th Floor, 58, Sahyog Building, Nehru Place, New Delhi-110019
Ph :011-45621761
Fax:011-45621761
Contact Person: Mr. Rohit Jain
Contact No.: 9911117635
E-mail :rohit[at]swadeshsystem.in

87. M/s Security Spoc LLP

Postal address: Level 18 Tower A, Building No. 5 DLF Cyber City Phase III, Gurgaon, Haryana,
122002 India
Ph : +918448866878, 01294900303
Contact Person: Dutt Kumar
E-mail: dkumar[at]securityspoc.com
Website: https://securityspoc.com

88. M/s TAC InfoSec Private Limited

C203, 4th Floor, World Tech Tower
Phase-8B, Mohali-160055
Ph : 9876200821, 9988850821
Contact Person: Mr. Trishneet Arora, Founder and CEO
E-mail: ceo[at]tacsecurity.co.in

89. M/s Tata Communications Ltd

Tower 4, 4th to 8th Floor, Equinox Business Park,
LBS Marg, Kurla (W), Mumbai 400070
Ph : +91 22 66592000
Contact Person: Mr.Ratnajit Bhattacharjee - DGM-GRC Product/Services
Mr.Saikat Sen - DGM Cyber Security Products
E-mail: Ratnajit.Bhattacharjee[at]tatacommunications.com,
Saikat.Sen[at]tatacommunications.com
Mobile: 9810093811, 7259308444

90. M/s Talakunchi Networks Pvt Ltd

Postal address: 505, Topiwala Centre,
Off S.V. Road, Goregaon West, Mumbai 400104
Phone: +91-9920099782
Contact Person: Vishal Shah
E-mail: certin[at]talakunchi.com

91. M/s Tata Advanced Systems Ltd.

Cyber & Physical Security Division
Postal address: Office No. 15, 6th floor, Tower 1,
Stellar IT Park, C-25, Sector-62 Noida, Uttar Pradesh, India. PIN - 201307
Fax: 0120 4847459
Contact Person: Argha Bose - (Head , Cyber Security Practice)
Email: argha.bose[at]tataadvancedsystems[dot]com
Mobile no.: 7028007432

92. M/s TUV-SUD south Asia Pvt. ltd

Solitaire, 4th Floor, ITI Road,
Aundh, Pune – 411007
Maharashtra
Ph : +91 20 6684 1212
Contact Person :Amit Kadam
E-mail:Amit.VKadam[at]tuvsud.com Phone:+91 9607964483
Mr. Vaibhav.Pulekar
E-mail:Vaibhav.Pulekar[at]tuvsud.com Phone: + 91-9819955909
Mr. Sivakumar Radhakrishnan,
E-mail:Sivakumar.R[at]tuvsud.com Phone: + 91-9819955909

93. M/s Tata Power Delhi Distribution Ltd

Tata Power Delhi Distribution Ltd, NDPL House,
Hudson Lane, New Delhi - 110009
Ph :01166112222
Fax:01127468042
Contact Person: Aamir Hussain Khan
E-mail:aamir.hussain[at]tatapower-ddl.com

94. M/s Varutra Consulting Varutra Consulting Private Limited

Postal address: Varutra Consulting Pvt. Ltd.,
West Wing, II Floor, Marigold Premises, Marisoft III,
Kalyaninagar ,411014 Pune ,Maharashatra, India.
Ph : +91 8408891911
Contact Person: Shrushti Sarode
E-mail:shrushti.sarode[at]infosharesystems.com

95. M/s Xiarch Solutions Private Limited

352, 2nd Floor, Tarun Enclave,
Pitampura, New Delhi-110034, India
Ph :011-45510033
Fax:011-66173033
Contact Person: Mr. Utsav Mittal, Principal Consultant
E-mail: utsav[at]xiarch.com, cert[at]xiarch.com

96. M/s Yoganandh & Ram LLP

G-1, Shree Vishnu Apartments, 12, Twelfth Cross Street,
Dhandeeswaram Nagar, Velachery, Chennai - 600042
Ph : 044-22432030
Contact Person: Mr. Manoj Kumar Jain
E-mail: manoj[at]yandr.in / isaudit[at]yandr.in
Mobile: 9940156515 / 98415 82933