Request for Proposal Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit

Tender Ref: WEBEL/EOT/COM/20-21/00072
Dated: 19-02-2021

Issued By:-
West Bengal Electronics Industry Development Corporation Limited (WBEIDCL)
Webel Bhawan, Block- EP & GP,
Sector-V, Salt Lake,
Bidhan Nagar,
Kolkata-700091,
West Bengal

Table of Content

Section-1: Key Information 5
a. Purpose of this RFP 5
b. Fact Sheet 5
Section-2: Background 8
a. Cyber Security Centre of Excellence Overview .... Error! Bookmark not defined.
b. **Objective of the project** 8
Section-3: Instruction to Bidders 9
Section-4: Scope of Work 13
4.1. Web application security audit, Vulnerability Assessment Services & Penetration Testing 13
4.2. Remediation Support 15
4.3. Procedure for Audit Activity 16
4.4. Scope of ICT Infrastructure Audit 16
4.4.1. Scope of Site Audit 16
4.5.3 Procedure for Audit Activity 18
Section-5: Invoicing & Payment Clauses 20
5.1. Invoicing 20
5.2. Payment Clause 20
Appendix 21
Appendix-2 : List of CERT-In empanelled Organisations 22
Annexure 23
Annexure I: Covering Letter for submission of RFP 23
Annexure II: Details of the Responding Bidder 24
Annexure III: Details of Projects undertaken 24
Annexure–IV: Format for Performance Bank Guarantee 25

Disclaimer

This Request for Proposal (RFP) contains brief information about the project, qualification requirements and the selection process for the successful applicant (bidder). The purpose of this RFP document is to provide applicants (bidders) with information to assist the formulation of their bid application (the "application").

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither West Bengal Electronics Industry Development Corporation Limited (WBEIDCL) , nor any of its officers or employees, nor any of their advisers accept any liability or responsibility for the accuracy, reasonableness or completeness of the information contained in the RFP, or for any errors, omissions or misstatements, negligent or otherwise, relating to the proposed project, or makes any representation or warranty, express or implied, with respect to the information contained in this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information ('Information') contained in this RFP document or subsequently provided to interested parties (the "applicant(s)), in writing by or on behalf of WBEIDCL is provided to applicant(s) on the terms and conditions set out in this RFP documents and any other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by WBEIDCL to any other party. The terms on which the project is to be developed and the right of the successful applicant shall be as set out in separate agreements contained herein. WBEIDCL reserves the right to accept or reject any or all applications without giving any reasons thereof. WBEIDCL will not entertain any claim for expenses in relation to the preparation of RFP submissions.

Abbreviations

Abbreviation	Description
API	Application Programming Interface
Auditee	Department or Owner of the application who is facing the audit/assessment
BID	Bugtraq ID
CERT	Computer Emergency Response Team
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
SI	Systems Integrator
SIEM	Security Information and Event Management
SME	Small and Medium Enterprise
SOC	Security Operations Centre
SPOC	Single Point of Contact
SQL	Structured Query Language
SSO	Single Sign On Computing
VA/PT	Vulnerability Assessment / Penetration Testing
WASA	Web Application Security Assessment
WBEIDCL	West Bengal Electronics Industry Development Corporation

Section-1: Key Information

a. Purpose of this RFP

West Bengal Electronics Industry Development Corporation Limited (WBEIDCL) invites RFP for Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit to cater different Government establishments and Cyber Security Centre of Excellence (CS-CoE) under the aegis of Department of IT & E, Govt. of West Bengal, **within the CERT-In Empanelled Information Security Auditing Organisations** to conduct Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit in West Bengal. Submission of RFP should be through electronic bidding process. The List of CERT-In Empanelled Information Security Auditing Organisations are available at https://www.cert-in.org.in/PDF/Empanel_org_2020.pdf.

b. Fact Sheet

1.	Tender No. & Date	**WEBEL/EOT/COM/20-21/00072 dated 19-02-2021**
2.	Tender Version	1.0
3.	Brief description of project	Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit
4.	Tender issuing entity	WBEIDCL
5.	Tender document Fee	Rs 1,000 (Rupees One thousand Hundred only) through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal. Digitally signed Technical Bid and Financial Bid, to be submitted through the website https://wbtenders.gov.in
6.	Earnest Money Deposit	The Bidder shall pay EMD of Rs. 35,000(Rupees Thirty Five Thousand Only) through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.
7.	Last Date and time of submission of the queries	**Date: 25-02-2021 at 4:00 PM**
8.	Pre-Bid Meeting (Online) Date , Time & Link	**Date 26-02-2021 at 12:00 PM** **Click here to Join Pre-Bid Meeting** (Microsoft Teams)
9.	Corrigendum (if any)	**Date: 01-03-2021**
10.	Bid Submission start date & time (online)	**Date: 02-03-2021 at 12:00 PM**

11.	Bid Submission closing date & time (online)	**Date: 05-03-2021 at 12:00 PM**
12.	Bid opening date & time for Technical Proposals (Online)	**Date: 08-03-2021 at 03:00 PM**
13.	Date of uploading the final list of Qualified Bidder to the website	**Date: To be notified later on**
14.	Queries may be sent to	1. Mr. Pratul Show, G.M.(Commercial & HR) E Mail: pratul.show@webel-india.com 2.Mr. Sourav Guha Thakurta G.M(CIO), sourav.guhathakurta@webel-india.com 3. Mr. Mainak Sen, Assistant Manager(IT) mainak.sen@webel-india.com 4. Mr. Kausik Halder, Assistant Manager (Com) halder.kausik@webel-india.com

Note: This document is not transferable

All Bidders are advised to check for any further clarifications and corrigendum related to this project at the website https://wbtenders.gov.in and https://www.webel.in .

Instruction to Bidders

A. Intending bidders may download the EoI document directly from the website https://wbtenders.gov.in .
B. Each bidder needs to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of EoI from the approved service providers on payment of requisite amount.
C. The digitally signed EoI response should be submitted in the website https://wbtenders.gov.in
D. Submission of RFP will be done as per time schedule stated mentioned in the Table 1 of this document.
E. For any queries regarding this RFP, please contact with WBEIDC Limited contact persons as mentioned in the Table 1 of this document on or before last date of submission of queries. No queries will be entertained after this timeframe.
F. RFP are to be submitted online to the website before the prescribed date & time using the Digital Signature Certificate (DSC). Virus scanned and duly digitally signed copies of the documents are to be uploaded.
G. In the event of e-filing, intending bidders may download the tender documents from the website https://wbtenders.gov.in directly. Necessary cost of tender documents (tender fees) of Rs. 1,000 (Rupees One Thousand Only) has to be remitted through Net banking or through RTGS NEFT through the https://wbtenders.gov.in //portal as per G.O 3975-F(Y) dated 28th July, 2016 issued by Finance department Govt. of West Bengal.
H. The bidder shall pay an EMD of Rs. 35,000 (Rupees Thirty Five Thousand only) through Net banking or through RTGS NEFT through the https://wbtenders.gov.in //portal as per G.O 3975-F(Y) dated 28th July, 2016 issued by Finance department Govt. of West Bengal.

I. Exemption under NSIC/ Udyog Aadhaar: - Bidders who are registered with NSIC, UNDER SINGLE POINT REGISTRATION SCHEME/ Udyog Aadhaar for the TENDERED ITEMS are exempted from payment of bid security and Tender Fees up to the amount equal to their monetary limit. A proof regarding current Registration with NSIC / Udyog Aadhaar for the TENDERED ITEMS will have to be attached and documented, otherwise the Bid will be treated as cancelled. In case of bidders having monetary limit as "NO LIMIT", the exemption will be limited to Rs.50, 00,000/- only as per existing policy of WBEIDC Ltd.

Section-2: Background

a. Introduction

West Bengal Electronics Industry Development Corporation Limited (WBEIDCL) invites RFP for Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit to cater different Government establishments and Cyber Security Centre of Excellence (CS-CoE) under the aegis of Department of IT & E, Govt. of West Bengal, **within the CERT-In Empanelled Information Security Auditing Organisations** to conduct Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit in West Bengal. Submission of RFP should be through electronic bidding process. The List of CERT-In Empanelled Information Security Auditing Organisations are available at https://www.cert-in.org.in/PDF/Empanel_org_2020.pdf.

b. Objective of the project

The main objective of this project is to appoint third-party auditing agency (ies) from the CERT-In empanelled Information Security Auditing Organisations, those will assist WBEIDC to perform different types of Web Application Security Audit & VAPT and ICT Infrastructure Audit for different Government establishments, to identify and mitigate vulnerabilities during assessment & provide recommendations to cope with that vulnerabilities. This will be the stepping stone towards Cyber Safe Bengal.

The Indicative Security Checks to be performed by the selected agency (ies) are mentioned below:

1. Application Code Testing
    a. Manual testing of code
    b. Automated testing of code
    c. Functional/controls audit
2. Web and Mobile Application Security Assessment
3. Internal & External Network Vulnerability Assessment
4. Internal & External Network Vulnerability Assessment Findings Closure Support
5. Penetration Testing for the production servers
6. Penetration Testing Findings Closure Support
7. Secure Configuration Review
8. Audit of ICT infrastructure

Section-3: Instruction to Bidders

a. Each bidder needs to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of RFP from the approved service providers on payment of requisite amount.

b. The digitally signed RFP response should be submitted in the website https://wbtenders.gov.in

c. Submission of RFP response will be done as per time schedule stated in this document.

d. This is an Open Tender. Only the CERT-In empanelled agencies will be eligible to participate in the tendering process.

e. For queries regarding this RFP, please connect with Mr. Pratul Show, G.M. (COMMERCIAL) E Mail: pratul.show@webel-india.com on or before last date of submission of queries. No queries will be entertained after this timeframe.

f. RFP responses are to be submitted online to the website before the prescribed date & time using the Digital Signature Certificate (DSC). Only the Digitally Signed documents are to be uploaded after proper virus scanning. The documents will get encrypted (transformed into non-readable formats).

g. No sub-contracting will be allowed.

h. Eligibility Criteria :- As per below mentioned Table

#	Basic Requirement	Eligibility Criteria	Document Proof
1.	Technical Requirement	• Bidder must be CERT-IN empanelled agency • Bidder should have licensed Application Audit and Server VA/PT Tool • Bidder should be ISO: 27001:2013 Certified Security Audit Lab	• CERT-IN registration document. • Copy of valid licenses for all Tools to be used needs to be attached • Copy of ISO: 27001:2013 Certificate
2.	Legal Entity	• The bidder should have existence in India for last three (3) years at the end of 31st March 2020. • The bidder shall be solvent at the date of bidding	• Certificates of incorporation for Company/ Partnership Deed / Proprietorship firm self-declaration • Certificate from Statutory auditor / Chartered Accountant for existence of firm for last three years along with last three years balance sheet. • Certificate from Statutory auditor / Chartered Accountant for Solvency declaration
3.	Work Experience	• The bidder should have executed at least 3 orders of similar nature of jobs, particularly in Cyber Threat & Vulnerability Assessment and web application Security Audit Services at any Govt. Department / Quasi Govt. Dept / PSU / Board / Council.	Order issued by the client + satisfactory certifications from client for ongoing projects. Managing Director or equivalent authorized signatory of the Consulting firm shall self-certify the projects if

			the firm has done assignments based on Non- disclosure Agreements and cannot share the contract / work-order.
4.	Other legal documents	• Trade License • GST Certificate • Income Tax Return (Latest 3 years) • Copy of PAN • Articles of Association/ Company Registration (depending on company type)	Copy of the valid documents
5.	Blacklisting	The responding firm must not be blacklisted by any Central/any State Department/establishments in India at any point of time for breach of ethical conduct or fraudulent practices.	A self-declaration that the bidder has not been blacklisted is to be submitted. In case it is found after issuing Work Order that the concerned organization is blacklisted by any Central/any State Department/establishments in India, the work order will be cancelled.
6.	Power of Attorney	The bidder shall submit the Power of Attorney of Authorization for signing the bid in Rs.100.00 Non Judicial Stamp Paper.	Scanned copy of Power of Attorney needs to be uploaded
7.	Submission of EMD	The Bidder shall pay EMD of Rs. 35,000 (Rupees Thirty Five Thousand only) through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.	To be submitted Online
8.	Submission of Tender Document Fee	Bidder should submit Tender Document Fee of Rs. 1,000 (Rupees One Thousand only) through net banking or through RTGS/NEFT in the portal of the website: https://wbtenders.gov.in as per G.O 3975-F(Y) dated 28th July 2016 issued by Finance Department, Govt. of West Bengal. For details regarding payment procedure & guideline on the same, bidders are advised to follow the mentioned order and portal.	To be submitted Online

i. RFP response should contain:

- ✓ This RFP document, with all pages signed by the authorized signatory
- ✓ Covering letter

- ✓ General information of the bidder
- ✓ The details of the project executed as per format mentioned in Annexure-III and Work Order copies along with job completion certificates from the customers duly attested.

j. The bidder shall bear all costs associated with the preparation and submission of the bid

k. The proposal will be prepared by the Bidder in English language only

l. **Consortium**: No Consortium is allowed in this bid. Declaration in this regard needs to be submitted.

m. **Evaluation Procedure** - The Tender Committee would perform the Commercial Evaluation for technically qualified bidders. The basis of price bid evaluation shall be "Least Cost Evaluation". L1 bidder will be selected on least overall rate quoted by the bidder.

n. **Rate Contract:** WBEIDC Ltd will reserve right to execute Rate Contract Agreement with the L1 bidder whose bid has been valued overall lowest as per Price for a period two(2) years or validity of Cert-In Empanelment period whichever is earlier. The contract will renewed based on satisfactory performance of the bidder(s) and validity of Cert-In Empanelment.

o. WBEIDC reserves the right not to accept the Lowest Price bid without assigning any reason what so ever and the bidder will not challenge such decision in any forum what so ever.

p. WBEIDC Ltd will also reserve right to execute Rate Contract Agreement with the bidders other than L1 bidder, if they agrees to match L1 rate.

q. **Award of Work Order**: Upon receipt of the order from the customer, WBEIDC reserves the right award the work to bidder(s) on round-robin basis. Bidder will not challenge such decision in any forum what so ever.

r. All decisions taken by the Tender Committee regarding the processing of this tender and award of contract shall be final and binding on all parties concerned.

s. The proposals shall remain valid till 180 days from bid submission date. During the period of validity of proposals, the rates quoted shall not change.

t. **Price of the Bid:** The prices shall be quoted in Indian Rupees only, inclusive of all applicable taxes. Price should be quoted in the Price Bid as per BOQ format only. No deviation in any form in the Price Bid sheet is acceptable.

u. **Confidentiality Agreement:**

1. In case of Web Application Security Audit, Vulnerability Assessment, Penetration Testing, the agency (ies) will maintain confidentiality of all data and information about the Web Application, system, Data & other resources obtained during the execution and will not reveal such information to any party without the prior written approval of WBEIDCL/Department of IT & E, Govt. of West Bengal. The Agency (ies) shall execute a overall Non-Disclosure Agreement for the duration Rate Contract with WBEIDCL before execution of Rate Contract Agreement.

2. In case of ICT Infrastructure Audit, the agency (ies) will maintain confidentiality of all data and information about the System, Data & other resources obtained during the execution and will not

reveal such information to any party without the prior written approval of WBEIDCL/Department of IT & E, Govt. of West Bengal. The Agency (ies) shall execute an overall Non-Disclosure Agreement for the duration Rate Contract with WBEIDCL before execution of Rate Contract Agreement referred in clause 1 above. The Agency (ies) has to submit a Non-Disclosure Declaration to the Government establishments on a case to case basis.

v. **Submission of PBG:** The successful agency (ies) shall furnish a Performance Bank Guarantee (PBG) amounting to Rs. 50,000(Fifty thousand only) to WBEIDCL for a period 2 years before execution of the Rate Contract within 7 days from the date of issuance of Letter of Intent. Failure to comply with the agreement shall constitute sufficient grounds for the forfeiture of the PBG. The PBG shall be released immediately after expiry of contract provided there is no breach of contract on the part of the bidder. No interest will be paid on the PBG.

Section-4: Scope of Work

4.1. Web application security audit, Vulnerability Assessment Services & Penetration Testing

The Bidder shall carry out assessments of public and private sector entities in West Bengal as per the list of entities mentioned in Appendix of the document with respect to the Information Security, Privacy and Continuity perspective. The Bidder would conduct assessment, subjected to permission of the relevant entities, to review the effectiveness of the processes and controls deployed by the entity under audit. The audit would be carried out across the following areas and methodology:

A. Web Application Security Assessment (WASA) : -

STEP-1: Check various web attacks and web applications for web attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to the website/Web-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.
- Other any attacks, which are vulnerability to the website and web applications

STEP-2: Re-Audit based on the Recommendations Report from Task 1

The vendor will be responsible to provide a detailed recommendations report for the vulnerabilities observed from Task 1.

STEP 3: Re-Audit, if required based on the Recommendations Report from Task 2 If vulnerabilities are observed form the re-audit, the vendor has to provide a detailed recommendations report on the vulnerabilities observed or found from Reaudit/ Task2. Webel is expected that all vulnerabilities will be removed at the Task 3 stage. The Audit firm/company has to submit a summary compliance report at end of each task and the final report should be certify that the website/web applications (should be mentioned the name of the website and/or web applications) is “Safe to Host”.

Deliverables and Audit Reports

A. The successful bidder will be required to submit the following documents after the audit for each website, as mentioned below and the audit firm must also submit suggestions / recommendations and other detailed steps for enhancing the website security.
    i. A detail report will be submitted with security status and discovered vulnerabilities, weaknesses and mis-configurations with associated risk levels and recommended actions for risk mitigations.
    ii. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary countermeasures and recommended corrective actions as recommended above need to be submitted in duplicate to the Webel. Also the same copy should be submitted to the concerned department.
    iii. All deliverables shall be in English language and A4 size format.
    iv. The vendor will be required to submit the deliverables as per agreed implementation Plan. The deliverables (like Summary compliance report, Check list, Audit Report, Executive Summary and Final compliance report after all observations) for each task to be submitted by the Auditors for this assignment as mentioned in the Task1, Task2 and Taks3.

B. Timeframe of the deliverables
    i. The selected successful bidder will be required to start the project within 3 days from the date of placing the order for the audit.
    ii. The entire audit must be completed within 30 days from placing of the order.
    iii. All the draft reports of the agreed deliverables should be submitted by the firm/company within 7 days of the commencement of the audit.
    iv. The successful bidder should submit the final reports of the deliverables within 20 days of the commencement of the audit or within 7 days of receiving feedback from the concerned department on draft reports.
    v. The audit, as mentioned above, has to be completed in time. It is expected that, if required, the successful bidder may deploy multiple teams to complete the audit projects within given time frame.

C. Audit Report

The Website security audit report is a key audit output and must contain the following:

a) Identification of auditee (Address & contact information)
b) Dates and Location(s) of audit
c) Terms of reference (as agreed between the auditee and auditor), including the standard for Audit, if any
d) Audit plan
e) Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents
f) Additional mandatory or voluntary standards or regulations applicable to the auditee

g) Standards followed Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
   - Tools used
   - List of vulnerabilities identified.
   - Description of vulnerability
   - Risk rating or severity of vulnerability
   - Test cases used for assessing the vulnerabilities
   - Illustration if the test cases to provide the vulnerability
   - Applicable screen dumps

h) Analysis of vulnerabilities and issues of concern

i) Recommendations for action

j) Personnel involved in the audit, including identification of any trainees

k) 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.

B. **Vulnerability assessment and Penetration testing (VAPT) of the IT infrastructure and network :-**
   - Vulnerability assessment and penetration testing for the Web Application and the entire IT network infrastructure.
   - The Vulnerability Assessment should be carried out at on-site for the devices/servers, etc and Penetration Testing should be carried out from the selected bidder's site. The VA/PT may also be carried out after obtaining written permission from Webel.
   - The selected bidder should complete the VA/PT activity and submit the reports within two weeks from the date of acceptance of Purchase Order.

Note:

The Bidder is required to perform a detailed security assessment for the assigned entity offering services. The Bidder is expected to prepare the audit checklist based on the responsibilities, risk and the information managed by the entity as well as the information security guidelines and controls defined by WBEIDCL from time to time. The audit shall be carried out after due approval and confirmation from WBEIDCL. The Bidder will maintain confidentiality of information received from the respective department/agencies, its eco system partners and assigned entity and no information will be shared with anyone other than designated personnel. All information, findings, documents will only be used for the purpose of audit as defined under scope of work in this document. The assessments have to be conducted as per the guideline of CERT-In and other security guidelines, notifications and requirements as prescribed by WBEIDCL from time to time.

4.2. Remediation Support

The empanelled agency will give remediation recommendations only to close the vulnerabilities and observations identified. Security issues that pose an imminent threat to the system are to be reported immediately.

4.3. Procedure for Audit Activity

1. On receipt of audit request from the department, WBEIDCL shall place order to the selected agencies on the basis of the roaster. The work order will have the details of SPOC of the auditee department.
2. On receipt of the work order, the Audit Agency will conduct the audit on the environment & identify vulnerabilities in the Application/Infrastructure as per industry standard.
3. WASA, MASA, Code Review, Functional controls Review shall be conducted on test environment. Test Environment should be ready before audit initiation and access shall be provided to agency by Department.
4. Code review to be conducted on-site on the department machine to avoid any source code misuse/leakage
5. VAPT, Configuration review shall be conducted on production environment. Downtime should be provided by Department.
6. Level 1 Interim report will be generated with details of vulnerabilities with recommendations for closing the discovered vulnerabilities.
7. Selected agency(ies) will submit the first level of audit report along with recommendations for closure in the mentioned SLA to be prepared by the agency
8. The SPOC will arrange for the implementation of recommendation from the selected agency and will request for confirmation of findings closure with selected agency.
9. Selected agency shall assist the auditee and reassess/rescan to validate the closure of findings.
10. The Selected agency will issue the Audit Compliance Certificate / Assurance certificate to the department post completion of the process if all the vulnerabilities are successfully patched.
11. There will be only 1 round of re-audit to verify the closure of findings from preliminary report submission.
12. WBEIDCL /Empanelled Agency is not be responsible for the audit if the fixing of the errors is not completed by the department within 2 months and intimated. Auditor shall perform assessment & reassessment within specified timelines.

4.4. Scope of ICT Infrastructure Audit

4.4.1. Scope of Site Audit

The agency has to perform site audit of all the entities as per the list mentioned in Appendix of the document. The agency has to perform following checks during site audit:

A. PHYSICAL

- Physical access to the site/premises
- Access to the site (for employees and visitors)
- Clear Screen/Clear Desk Policy
- Security of equipment/documents onsite
- Active list of users working currently at the site (also access of those who have left)
- Appropriate usage of recording devices (camera, smartphones, etc.) to avoid data leakage
- Cabling Security for Network cables, power cables, etc.

B. ENVIRONMENTAL

- Appropriate equipment for protection of critical infrastructure (e.g. AC)
- Power backup mechanisms are available and maintained
- Appropriate temperature and moisture content is being maintained inside

C. ASSET

- Asset inventory including documentation, tagging of assets, etc.
- Physical condition of asset like age, wear and tear, AMC, etc.
- Logging mechanisms of movement of assets in and out of the site

D. ENDPOINT

- Operating System should not be beyond end of life support by OEM
- OS is hardened
- Personal firewall
- User Access Management (including password policy)
- Admin roles are restricted
- Port blocking to prevent data leakage using pen drive, Bluetooth, NFC, etc.
- Applications installed in the systems adhere to the software policy and are updated regularly
- Physical security of mobile/portable devices
- Backup procedure
- Batch/scheduled job monitoring
- Password policy
- Use of malicious web sites
- Secure logon and logoff procedure
- Antivirus

E. USER

- User has basic knowledge of common cyber threats

4.5.2 State IT Infrastructure Audit Framework

a) Phase I – Walk through/ reconnaissance
   i) The first phase of IT Infrastructure Audit is the reconnaissance or walkthrough of the premises. This activity would comprise of the following steps –
   ii) Physical observation of apparent vulnerabilities
   iii) High level risk assessment – cyber security risks observable at first glance
   iv) Discussion with process owners to discover observable major cyber security loopholes
   v) Cursory examination of information systems to check for observable vulnerabilities
   vi) High level review of available policy, process and procedural documents
   vii) Based on the observations recorded during the walkthrough process, the level of cyber security preparedness can be classified into the following categories –

b) Critical –
   i) In depth audit required of all people, processes and technology aspects in the department.
   ii) Vulnerabilities discovered during the walkthrough process to be flagged/ labelled into urgent and important depending on probable impact. Enabling prioritization of the audit process.
   iii) Cyber security training of staff to enable them to comprehend the importance of maintaining cyber hygiene in the work place.
   iv) Handholding of system administrators and other staff to enable mitigation of major cyber security gaps identified during the walkthrough process.

c) Not in order –
   i) Thorough audit is required. Some modules from a system, process or people perspective would typically require detailed audit whereas some security controls would already be in place – not requiring thorough audit.
   ii) Vulnerabilities discovered during the walkthrough process to be flagged/ labelled into urgent and important depending on probable impact. Enabling prioritization of the audit process.
   iii) Cyber security training of staff to enable them to comprehend the importance of maintaining cyber hygiene in the work place.
   iv) Handholding of system administrators and other staff to enable mitigation of major cyber security gaps identified during the walkthrough process.

d) Phase II – Audit
   i) Based on the observations/ findings discovered during Phase I, phase II would consist of the following steps –
   ii) Requisition for Audit/ Letter of Intent from the department concerned to onboard vendor for internal audit.
   iii) Conduct detailed risk assessment and audit based on defined standard and findings of phase I.
   iv) Publish detailed audit report
   v) System administrators and staff to be trained on mitigation of the security gaps identified and achieving compliance.

e) Phase III – Implementing reforms
   i. Achieving the following compliances –
   ii. Hardware compliance – meeting the hardware requirements to address the gaps identified in the internal audit.
   iii. Process compliance including publication of Software Operating Processes (SOP)
   iv. System compliance – Mitigating any identified vulnerabilities
   v. Application compliance – ensuring all user level data and web services are error free

f) Phase IV – Third Party Audit and Certification

Third Party Audit and Certification to be carried out by an enlisted and independent body. Any party involved in Phases I to III above are not eligible to carry out third party certification.

4.5.3 Procedure for Audit Activity

a) On receipt of audit request from the department, WBEIDCL shall place order to the selected agencies. The work order will have the details of SPOC of the department/organization to be audited.
b) On receipt of the work order, the Audit Agency will conduct the first phase of IT Infrastructure Audit is the reconnaissance or walkthrough of the premises & identify vulnerabilities in the Application/Infrastructure as per industry standard.
c) IT Infrastructure Audit for phase 1 audit report will be generated with details of vulnerabilities with recommendations for closing the discovered vulnerabilities with recommendations for closure and will be submitted to auditee department with a copy to WBEIDC.
d) Thereafter agency will make necessary communication with auditee department/organization for quick initiation of Phase II audit.
e) On receipt of Phase II audit request from the department, WBEIDCL shall place order to the same agency.

f) On receipt of the work order, the Audit Agency will conduct the Second phase of IT Infrastructure Audit & identify vulnerabilities in the Application/Infrastructure as per industry standard.

g) IT Infrastructure Audit for phase II audit report will be generated with details of vulnerabilities with recommendations for closing the discovered vulnerabilities with recommendations for closure and will be submitted to auditee department with a copy to WBEIDC

h) The SPOC will arrange for the implementation of recommendation from the selected agency and will request for confirmation of findings closure with selected agency as part of Phase III – Implementing reforms

i) Selected agency shall assist the Phase III – Implementing reforms for auditee and reassess/rescan to validate the closure of findings.

j) After successful implementation of reforms by the auditee department/organization the selected agency will issue the Audit Compliance Certificate / Assurance certificate to the department/organization post completion of the process if all the vulnerabilities are successfully patched.

WBEIDCL /Empaneled Agency is not be responsible for the audit if the fixing of the errors is not completed by the department within 2 months and intimated. Auditor shall perform assessment & reassessment within specified timelines

Section-5: Invoicing & Payment Clauses

5.1. Invoicing

The auditor has to complete the audit activity as per the clause mentioned in the order issued to them. After issuance of the Safe to Host Certificate/Safe to Go Live certificate, the auditor may raise invoice in favour of WBEIDC Ltd.

5.2. Payment Clause

- For Clients of WBEIDC payments shall be made within (30) days against receipt of the payment from the end customer & against submission of invoices & Safe to Host Certificates
- For WBEIDC's own audit activity, payments shall be made within (30) days & against submission of invoices & Safe to Host Certificates
- Further all payments to agency will be made subject to deduction of TDS (Tax deduction at Source) as per the income Tax Act, 1961, applicable penalty and other taxes, if any, as per Government of India rules.

Appendix

Appendix-1: Unpriced BOQ

Web Application Security Audit, VA & PT

Sl. No.	Item Description
1.	Web Application Security Audit – Static Application
2.	Web Application Security Audit – Dynamic Application (1 – 25 fields)
3.	Web Application Security Audit – Dynamic Application (26 – 100 fields)
4.	Web Application Security Audit – Dynamic Application (101 – 200 fields)
5.	Web Application Security Audit – Dynamic Application (More than 200 fields)
6.	Vulnerability Assessment of a Physical Server
7.	Vulnerability Assessment of a Virtual Server
8.	Penetration testing of a Physical Server
9.	Vulnerability Assessment of a Virtual Server
10.	Web Application Security Audit for 1 year (Audit will be done every quarter. No Field count limitation)

ICT Infrastructure Audit

Sl. No.	Item Description
1.	ICT infrastructure with 20 end points
2.	ICT infrastructure with 21 to 50 end points
3.	ICT infrastructure with 51 to 100 end points
4.	ICT infrastructure with 101 to 200 end points
5.	Network Security Audit having less than 10 end points
6.	Network Security Audit having more than 10 end points

Appendix-2: List of CERT-In empanelled Organisations

The List of CERT-In empanelled IT Security Auditing Organisations may be viewed from the following link:

https://www.cert-in.org.in/PDF/Empanel_org_2020.pdf

Annexure

Annexure I: Covering Letter for submission of RFP

(To be submitted on the letterhead of the bidder)

(Date)

To,

General Manager (Commercial),

WBEIDC,

Webel Bhavan, Block-EP & GP, Sector-V,

Salt Lake, Bidhan Nagar, and Kolkata:-700091

Ref: WEBEL/EOT/COM/20-21/00072

Sub: Submission of RFP for "Request for Proposal Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit"

Dear Sir/Madam,

We have examined the RFP document, we, the undersigned, herewith submit our RFP in response to your RFP no. WEBEL/EOT/COM/20-21/00072 dated 19-02-2021 for "Request for Proposal Selection of Agency (ies) for Rate Contract of Web Application Security Audit, Vulnerability Assessment, Penetration Testing and ICT Audit", in full conformity with the said RFP document.

i. We have read the provisions of the RFP document and confirm that these are acceptable to us. We further declare that additional conditions, variations, deviations, if any, found in our RFP shall not be given effect to.
ii. We agree to abide by this RFP, consisting of this letter, the detailed response to the RFP and all attachments, for a period of 180 days from the date of submission of the bid.
iii. We would like to declare that we are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this assignment and we are not under a declaration of ineligibility for corrupt or fraudulent practices
iv. We would like to declare that there is no conflict of interest in the services that we will be providing under the terms and conditions of this RFP.
v. We hereby declare that all the information and statements made in this RFP are true and accept that any misrepresentation contained in it may lead to our disqualification.
vi. We understand you are not bound to shortlist / accept any RFP you receive

Sincerely,

Signature of Authorized Signatory and Seal of the bidder

Name:

Designation:

Date:

Annexure II: Details of the Responding Bidder

#	Description	Details (to be filled by the responder to the Bid)
1.	Name of the company	
2.	Official address	
3.	Phone No. & Fax No.	
4.	Corporate Headquarters Address	
5.	Phone No. & Fax No.	
6.	Web Site Address	
7.	Details of Company's Registration (Please enclose copy of the company registration document)	
8.	Name of Registration Authority	
9.	Registration Number and Year of Registration	
10.	CERT –In Empanelled Certificate	
11.	GST Registration No.	
12.	Permanent Account Number (PAN)	
13.	Company's Revenue for last 3 years (Year wise)	
14.	Company's net worth for the last year	

Annexure III: Technical Details of Bidder

#	Technical Valuation Details	Values
1.	Describe Experience in working with Government Departments and Public Sector for similar Projects.	
2.	Describe Quality Management Standards/Certifications	
3.	Describe Experience in conducting similar website and web application Security Audit.	
4.	Describe Level of understanding of the Project	
5.	Type of Security assessment tool will be used for identifying Security Vulnerabilities (Licensed /Free) and Technologies.	
6.	List Number of CISA / CISSP and other personnel to be deployed on this project. a) No of CISAs :- b) No of CISSPs:- c) Others:-	
7.	Sample Audit reports	

Annexure–IV: Format for Performance Bank Guarantee

(On non-judicial stamp paper of appropriate value to be purchased in the name of executing Bank)
Proforma of Bank Guarantee for Security Deposit cum Performance Guarantee

Ref ..... Bank Guarantee no.....
Date.....

PROFORMA OF BG FOR SECURITY DEPOSIT KNOW ALL MEN BY THESE PRESENTS that in consideration of WBEIDC Ltd, a Government of West Bengal Enterprise under the Department of Urban Development, Govt. of West Bengal having its registered office at Webel Bhawan, Block- EP & GP, Sector-V, Salt Lake, Bidhan Nagar, Kolkata-700091, (hereinafter called "The Purchaser") having agreed to accept from _____(hereinafter called "The empanelled agency") Having its Head Office at _____, a Bank guarantee for Rs. _____ in lieu of Cash Security Deposit for the due fulfilment by the firm of the terms & conditions of the Work Order No. _____dated_____ issued by the Purchaser for _____(hereinafter called "the said work order _____dated_____)". We _____ (Name & detailed address of the branch) (hereinafter called "the Guarantor") do hereby undertake to indemnify and keep indemnified the Purchaser to the extent of Rs._____ (Rupees _____) only against any loss or damage caused to or suffered by the Purchaser by reason of any breach by the firm of any of the terms and conditions contained in the said Work Order No. _____ dated_____ of which breach the opinion of the Purchaser shall be final and conclusive.

(2) AND WE, _____DO HEREBY Guarantee and undertake to pay forthwith on demand to the Purchaser such sum not exceeding the said sum of _____Rupees_____) only as may be specified in such demand, in the event of the firm failing or neglecting to execute fully efficiently and satisfactorily the order for _____ Work Order no. , _____dated _____

(3) We _____ further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said order as laid down in the said Work Order No. _____ dated _____ including the warranty obligations and that it shall continue to be enforceable till all the dues of the Purchaser under or by virtue of the said Work Order No. _____ dated _____ have been fully paid and its claims satisfied or is charged or till the Purchaser or its authorized representative certified that the terms and conditions of the said Work Order No. _____ dated _____ have been fully and properly carried out by the said firm and accordingly discharged the guarantee.

(4) We _____the Guarantor undertake to extend the validity of Bank Guarantee at the request of the firm for further period of periods from time to time beyond its present validity period failing which we shall pay the Purchaser the amount of Guarantee.

(5) The liability under the Guarantee is restricted to Rs. _____ (Rupees _____) only and will expire on _____and unless a claim in writing is presented to us or an action or suit to enforce the claim is filled against us within 6 months from _____ all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities (thereinafter)

(6) The Guarantee herein contained shall not be determined or affected by liquidation or winding up or insolvency or closer of the firm.

(7) The executants has the power to issue this guarantee on behalf of Guarantor and holds full and valid power of Attorney granted in his favour by the Guarantor authorizing him to execute the Guarantee.

(8) Notwithstanding anything contained herein above, our liability under this guarantee is restricted to Rs. _____ (Rupees _____) only and our guarantee shall remain in force up to _____ and unless a demand or claim under the guarantee is made on us in writing on or before _____ all your rights under the guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.

WE, _____lastly undertake not to revoke this guarantee during the currency except with the previous consent of the Purchaser in writing. In witness whereof we _____have set and subscribed our hand on this _____ day of _____.

SIGNED, SEALED AND DELIVERED

_____

(Stamp of the executants)

WITNESS

1) _____

2) _____

(Name & address in full with Rubber Stamp)

INSTRUCTIONS FOR FURNISHING BANK GUARANTEE

1. B.G. for security Deposit-cum-Performance Guarantee, Earnest Money should be executed on the Non- Judicial Stamp paper of the applicable value and to be purchased in the name of the Bank.
2. The Executor (Bank authorities) may mention the Power of Attorney No. and date of execution in his/her favour with authorization to sign the documents. The Power of Attorney is to be witnessed by two persons mentioning their full name and address.
3. The B.G. should be executed by a Nationalised Bank/ Scheduled Commercial Bank preferably on a branch located in Kolkata. B.G. from Co-operative Bank / Rural Banks is not acceptable.
4. A Confirmation Letter of the concerned Bank must be furnished as a proof of genuineness of the Guarantee issued by them.
5. Any B.G. if executed on Non-Judicial Stamp paper after 6 (six) months of the purchase of such stamp shall be treated as Non-valid.
6. Each page of the B.G. must bear signature and seal of the Bank and B.G. Number.
7. The content of the B.G. shall be strictly as Proforma prescribed by WBEIDCL Ltd. in line with Purchase Order /LOI/ Work Order etc. and must contain all factual details.
8. Any correction, deletion etc. in the B.G. should be authenticated by the Bank Officials signing the B.G.
9. In case of extension of a Contract the validity of the B.G. must be extended accordingly.
10. B.G. must be furnished within the stipulated period as mentioned in Purchase Order / LOI / Work Order etc.
11. Issuing Bank / The Vendor are requested to mention the Purchase Order / Contract / Work Order reference along with the B.G. No. For making any future queries to WBEIDC LTD.