BIHAR STATE ELECTRONICS DEVELOPMENT CORPORATION LIMITED

CIN-U31900BR1978SGC001317

(A Govt. of Bihar Undertaking)

Ref. No. : 7794/2020

Date : 24/12/2020

To,

All Cert-In empanelled vendors

Sub.: Regarding selection of security auditor for website/application, mobile application and SSL certificate.

Sir,

With reference to the above mentioned subject, this is to inform you that, Bihar State Electronics Development Corporation Limited is willing to select auditor for security audit of website/application, mobile application and SSL certificate.

The scope of work and other details are mentioned in the attached Terms of Reference (ToR). You are requested to submit your technical and financial bids in two separate envelopes on the address mentioned in the attached ToR. The last date of bid submission is 22 January 2021.

Thanking You,

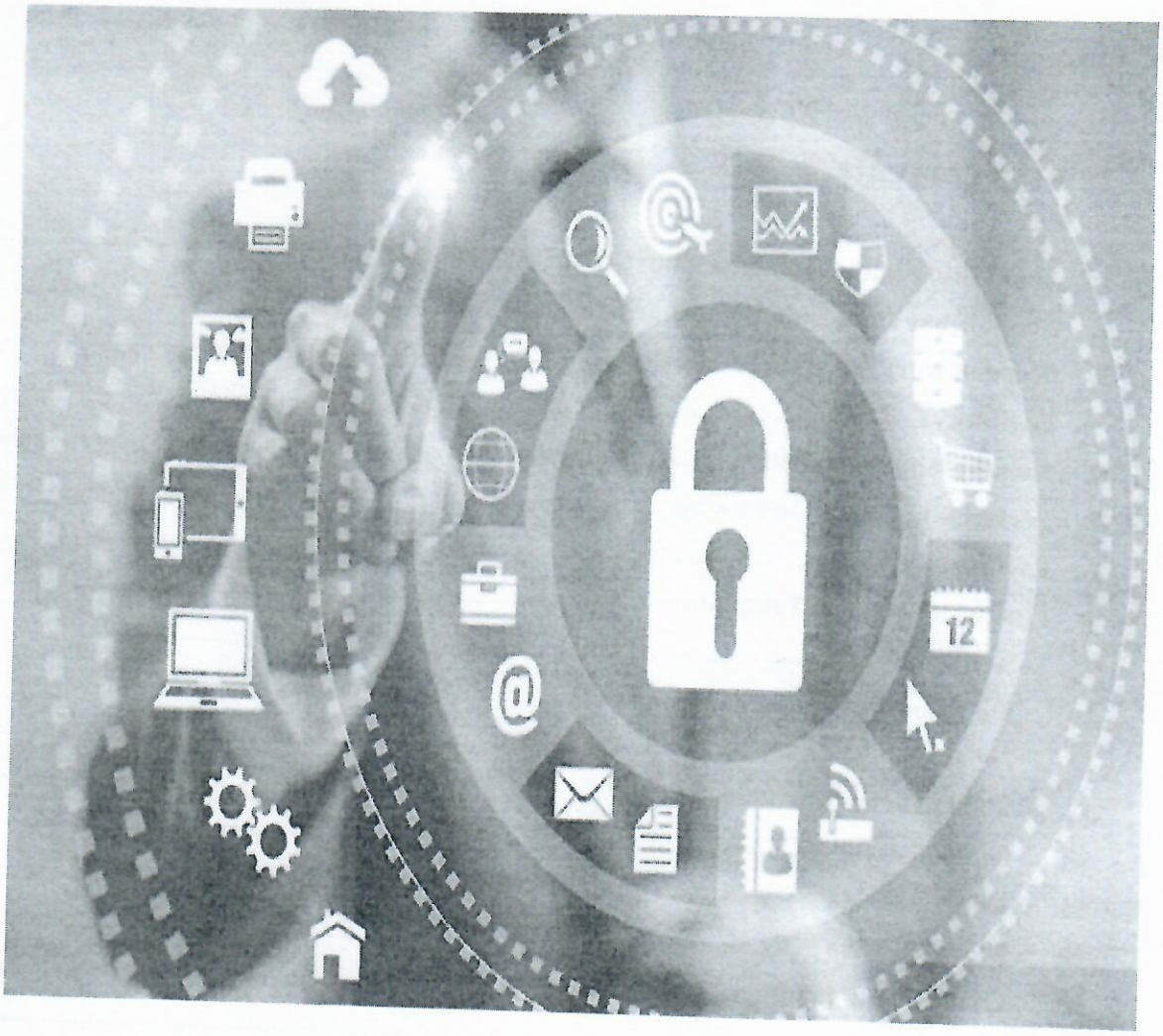
Yours faithfully

24/12

(Santosh Kumar Mall)
Managing Director

Enclosure: Terms of Reference

Term of Referenc for "Selectionof security auditor for Website, application and SSL certificate



ToR Ref No./BSEDC/...7794.../2020

Dated: 24/12/2020

Bihar State Electronics Development Corporation Limited
(A Government of Bihar Undertaking)
Beltron Bhawan, Shastri Nagar, Patna, Bihar
Pin: - 80023 Tel: 0612 – 2281857, 2281856 Fax: 0612- 2281857
Contact Person: Sujeet Kumar
Email id: Sujeet.Kumar@bihar.gov.in

35

Table of Contents

1. About Bihar State Electronics Development Corporation Limited

Bihar State Electronics Development Corporation Ltd. (BSEDC) is the nodal agency of the Bihar state working towards promotion & implementation of IT and e-Governance. It is the single point of access to any IT business opportunity in Bihar and encourages various players in the field of IT to come forward and invest in the state of Bihar.

BSEDC is committed to generate IT business for the public/private sector with a mandate from the Government to develop IT in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, IT training and an entire gamut of direct and indirect IT businesses.

2. About Bihar State Data Centre:

State Data Centre is the shared, reliable and secure infrastructure service centre for hosting and managing the e-Governance Applications of State and its constituent departments. SDC is envisaged to establish a robust infrastructure to enable the Government to deliver the services quickly and effectively to its stakeholders.

The State Data Centre is a key-supporting element of e-Government Initiatives &businesses for delivering services to the citizens with greater reliability, availability and service ability. SDC will provide better operations & management control and minimize overall cost of Data Management, IT Management, Deployment and other costs. State Data Centre acts as a mediator and convergence point between open unsecured public domain and sensitive government environment. It enables various State departments to host their services/applications on a common infrastructure leading to ease of integration and efficient management, ensuring that computing resources and the support connectivity infrastructure is adequately and optimally used. Applications of various department of Government of Bihar are hosted at data centre

3. Scope of work for security auditor:

Bihar State Electronics Development Corporation Limited (BSEDC) is willing to select security auditor for below mentioned scope of work for the period of 3 years. The scope of work includes following but is not limited to:

A. **Website and application security**
B. **Security audit of mobile application**
C. **Providing SSL certificate**
D. **Submission of "Safe to host" certificate**

A. Website and application security:

The assessment should cover both business logic and technical risks. The list of applications /website with all required inputs shall be shared with successful bidder.

Technical assessment:

- The assessment report should contain a detailed threat list of the application.
- The threat list should contain the possible risks to the application both from a business and technical aspect
- The tester should attempt to identify and exploit vulnerabilities that include the OWASP Top 10, including:

  o Input validation
  o Cross site scripting
  o SQL and XSL injection
  o Cookie modification
  o Code execution
  o Buffer overflow
  o URL manipulation
  o Authentication bypass
  o File upload vulnerabilities
  o Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
  o Session hijacking
  o CSRF
  o Privilege escalation

- The report should show risk to the business based on any exploits found.
- The assessment report should contain a test plan that shows what tests were conducted and its status.

Process Assessment

Authorization and Segregation of Duties Controls:

- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Perform sample testing of user application entitlement to ensure access to enter, approve, and /or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- Populate issue and findings log with the gaps / deviations / issues noted (if any)

Assessment of Role based Security for Applications under scope:

- Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
- Review of privileged access rights granted to application, system administrators, service providers and vendors
- Assess the process for review of user logs for administrator and system users
- Review ongoing monitoring of effectiveness of implemented procedures and controls
- Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel.
- Review of account and password policy including controls such as
    - Users are assigned unique accounts
    - Adequate passwords are maintained e.g. alphanumeric, minimum number of characters. etc
- Periodic password changes an o Review of implementation of password policy at system and application levels
- Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
- Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles/ profiles.
- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of application's entitlements to confirm appropriate segregations of duties are being enforced by the system (in a test environment)
- Understand how unsuccessful access attempts to applications in scope are logged and monitored preventing repeated use of passwords

Note: Bidder may perform vulnerability assessment from offsite; however; in case bidder face any network connectivity issue, they have to came to Bihar State Data Centre in order to perform the activity. BSEDC shall not pay any out of pocket (OPE) expenses like travel, food, accommodation, tool licenses etc.

B. Security audit of mobile application:

Identify and verify the mobile application security vulnerabilities against industry global standards such as OWASP, PCI compliance, RBI, UIDAI etc.The list of mobile applications with all required inputs shall be shared with agencies post empanelment.

- Perform assessments to identify vulnerabilities that can be exploited using applications on mobile phones for both registered and anonymous users
- Understand the features, functions in the application
- Perform automated and manual tests like, SQL Injection, Session Hijacking, LDAP Injection, Authentication Bypass etc.

31

- Check Adherence to Operational/Statutory guidelines issued by Regulatory bodies w.r.t Mobile Banking Application Perform audit of various functionalities provided in the application
- Perform verification of the detailed security procedures & processes of the Mobile Banking Solution provider as a part of the existing operational rules & regulations covering transaction, Data & Operational Security setup & establishing the adequacy of the same w.r.t the current Setup.
- Check adequacy Of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Audit ability etc. for the Mobile Application Solution
- Conduct audit of various security features including but not limited to Handset Security features, Transaction level security features, Platform Security & reliability features including Database, Network & transmission Security features, Registration features, Administration Portal features, Call logging, tracking & Dispute Resolution features etc

C. Providing SSL certificate:

Selected bidder has to provide SSL certificate for the website on request of BSEDC.

D. Submission of "Safe to host" certificate:

Post mitigation of all vulnerabilities of website/application/mobile application, selected bidder has to provide "safe to host" certificate to BSEDC.

4. Eligibility Criteria:

Sl. No.	Eligibility Criteria	Documents Required
1	Bidder must be CERT-IN empanelled agency for the last Eight (8) years(including date of bid submission)	Certificate of empanelment with CERT-In
2	Turnover of the bidder shall not be less than 1.5 crores in the each last three years i.e. 2017-2018, 2018-2019 and 2019-2020	CA certified balance sheet
3	The bidder should have existence in India for last five (5) years	1) Certificates of incorporation for Company 2) Registered office address proof
4	Other legal documents: 1) ST Certificate	Copy of the valid documents

Sl. No.	Eligibility Criteria	Documents Required
	2) Copy of PAN	
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 submitted
7	Bidder should have at least five (5) resources each for below mentioned certifications. 1) CISSP/CISA/CISM 2) CEH 3) CCNA 4) CCNP	CV of resources with scan copy of certification dully vetted by organisation HR and authorised signatory
8	Work Experience The bidder should have executed at least 5 orders of similar nature of jobs, particularly in Vulnerability Assessment, Site Security Audit and mobile application security audit Services at any Govt. Department / PSU /banking	1) Order issued by client 2) Authorised signatory of the bidder shall self-certify the project if the firm has done the assignment based on Non-disclosure agreement
9	Work Experience The bidder should have executed at least 3 orders of similar nature of jobs, particularly in Vulnerability Assessment, Site Security Audit and mobile application security audit Services at any Govt. Department / PSU /banking and value of each order shall not be less than 10 lakhs	1) Work order / Purchase order issued by client
10	The bidder must be ISO 27001:2013 certified	Scan copy of ISO 27001:2013 certificate

29

5. Earnest Money Deposit:

Rs. 1,00,000.00/- (One Lakh only) in form of Bank Guarantee in favour of "Bihar State Electronics Development Corporation Limited" payable at Patna from a nationalized / scheduled commercial bank in India.

6. Performance Bank Guarantee:

Successful bidder must submit PBG @ 10% of the total project value after award of contract.

7. Payment Terms:

a) Website and application security:

Sl. No.	Item Description	Report submission (in days)	% of payment shall be released
1	Submission of draft report post receiving the work order/purchase order to BSEDC and Department/Society/Mission etc	30 days	50 % of the work order/purchase order will be released
2	Re-scan of website/application and submission of final report along with "safe to host" certificate after 30 days from the time of submission of draft report to BSEDC and Department/Society/Mission etc	30 days	50 % of the work order/purchase order will be released
Note: Selected bidder needs to assist Department/Society/Mission etc. in order to close the highlighted vulnerabilities. In case after two scans vulnerability has not been closed by Department/Society/Mission, then in case more scans are need, bidder will be paid on per scan basis.			

b) **Security audit of mobile application:**

Sl. No.	Item Description	Report submission (in days)	% of payment shall be released
1	Submission of draft report post receiving the work order/purchase order to BSEDC and Department/Society/Mission etc	30 days	50 % of the work order/purchase order will be released
2	Re-scan of mobile application and submission of final report after 30 days from the time of submission of draft report to BSEDC and Department/ Society/Mission etc	30 days	50 % of the work order/purchase order will be released
Note: Selected bidder needs to assist Department/Society/Mission etc. to close the highlighted vulnerabilities. In case after two scans vulnerability has not been closed by Department/Society/Mission, then in case more scans are need, bidder will be paid on per scan basis.			

c) **Providing SSL certificate:**

Sl. No.	Item Description	Report submission (in days)	% of payment shall be released
1	Submission and installation of SSL certificate	10 days	100 % of the work order/purchase order will be released after submission and successful installation of SSL certificate
Note: Selected bidder needs to assist Department/Society/Mission etc. in installing the SSL certificate.			

27

8. Financial Proposal Template

Sl. No.	Item Description	A	B	C
		Unit Price (INR)	Tax amount (INR)	Total amount (A+B)
1	Security audit of website/application			
2	Security audit of mobile application			
3	SSL certificate having validity of one year			

Sl. No.	Item Description (Rescan after two scans in case vulnerability has not been closed by department/mission/society)	A	B	C
		Unit Price (INR)	Tax amount (INR)	Total amount (A+B)
1	Unit scan cost for website/application			
2	Unit scan cost for mobile application			

9. Selection Method:

BSEDC shall select successful bidder on Least Cost Method (L1)

10. Bid Submission:

Bidder must submit hardcopy of their technical and financial bid in two separate envelopes to below mentioned address. Bidder must mention the ToR reference no. and title on the envelopes.

To,

Managing Director,
Bihar State Electronics Development Corporation Limited,
Beltron Bhawan, Shastri Nagar,
Patna (Bihar), Pin Code: 800023

11. Penalty:

In the event of delayed delivery of the deliverables for more than one (1) month, **solely due to bidder,** penalty of 10% of purchase order/work order value shall be imposed. Post delay of one (1) month, additional penalty (other 10% of purchase order/work order) of Rs.5,000.00 shall be imposed per week. Deliverables and timeline shall be as per section 8.

12. Right of Selection/Rejection

Waiver of Informalities or Irregularities BSEDC reserves the right to reject any or all proposals, to waive any minor informalities or irregularities contained in any proposal, and to accept any proposal deemed to be in the best interest of the Department. Selection of a vendor solution shall not be construed as an award of

contract, but as a commencement of contract negotiation, including but not limited to the contract price proposed.

13. Confidentially

As used herein, the term "Confidential Information" means any information, including information created by or for the other party, whether written or oral, which relates to internal controls, computer or data processing programs, algorithms, electronic data processing applications, routines, subroutines, techniques or systems, or information concerning the business or financial affairs and methods of operation or proposed methods of operation, accounts, transactions, proposed transactions or security procedures of either party of any of its affiliates, or any client of either party, except such information. It is the express intent of the parties that all the business process and methods used by the Bidder in rendering the services here under are the Confidential Information of the Bidder.

The Bidder shall keep confidential any information related to this tender with the same degree of care as it would treat its own confidential information. The Bidders shall note that the confidential information will be used only for the purposes of this tender and shall not be disclosed to any reason whatsoever.

At all times during the performance of the Services, the Bidder shall abide by all applicable security rules, policies, standards, guidelines and procedures. The Bidder should note that before any of its employees or assignees is given access to the Confidential information, each such employee and assignees shall agree to be bound by the term of this tender and such rules, policies, standards, guidelines and procedures by its employees or agents.

The Bidder should not disclose to any other party and keep confidential the terms and conditions of this Contract agreement, any amendment hereof, and any Attachment or Annexure hereof.

25

14. Arbitration

BSEDC and the selected bidder shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the Contract. If, after thirty (30) days from the commencement of such informal negotiations, BSEDC and the selected Bidder have been unable to amicably resolve dispute, either party may require that the dispute be referred for resolution to the formal mechanisms, which may include, but are not restricted to conciliation mediated by a third party acceptable to both, or in accordance with the Arbitration and

Conciliation Act, 1996. All Arbitration proceeding shall be held at Patna, Bihar State, and the language of the arbitration proceeding and that of all documents and communications between the parties shall be in English.

15. Force Majeure

Neither party shall be responsible to the other for any delay or failure in performance of its obligations due to any occurrence commonly known as Force Majeure which is beyond the control of any of the parties, including, but without limited to, fire, flood, pandemic (declared by government), explosion, acts of God or any Governmental body, public disorder, riots, embargoes, or strikes, acts of military authority, epidemics, strikes, lockouts or other labor disputes, insurrections, civil commotion, war, enemy actions. If a Force Majeure arises, the Bidder shall promptly notify Tendered in writing of such condition and the cause thereof. Unless otherwise directed by Tendered, the successful bidder shall continue to perform his obligations under the contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. The successful bidder shall be excused from performance of his obligation in whole or part as long as such causes, circumstances or events shall continue to prevent of delay such performance.

16. Limitation of Liability:

Client (and any others for whom Services are provided) shall not recover from bidder, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Client (and any others for whom Services are provided)

shall not recover from bidder, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services.

17. Termination:

Either Party may terminate this Agreement immediately by giving notice of three (3) months to the other party. Upon termination bidder shall be entitled to receive payments of the Services performed, work in progress and expenses incurred by it, till the date of such termination.