National Backward Classes Finance & Development Corporation
5th Floor, NCUI Building, 3, Siri Institutional Area, August Kranti Marg, New Delhi-110016
Tel: +91-11-45854400, E-mail: nbcfdc@del3.vsnl.net.in

(Tender/Bid Document)

(Invitation of sealed quotations from CERT-IN empanelled agencies for security audit of NBCFDC Website and Loan & Employee Information Automation Project (LEAP) Software)

No: NBCFDC/IT/WebSecurityAudit//2017   **Dated: 27.09.2017**

1.   About NBCFDC

National Backward Classes Finance & Development Corporation (NBCFDC) is a Govt. of India Undertaking under the aegis of Ministry of Social Justice and Empowerment**.** NBCFDC was incorporated under Section 25 of the Companies Act 1956 on **1**3th January 1992 as a Company not for profit with an objective to promote economic and developmental activities for the benefit of Backward Classes and to assist the poorer section of these classes in skill development and self-employment ventures. NBCFDC provides financial assistance through State Channelizing Agencies (SCAs) nominated by the respective State Governments/UTs and Regional Rural Banks, Public Sector Banks. The Corporation supports a wide range of income generating activities to assist the poorer section of these classes in skill development and self-employment ventures.

2.   Tender/Bid Objective

NBCFDC invites techno commercial quotes from **CERT-IN empanelled agencies** on two bid system for selection of vendor for IT Security Audit Certification for NBCFDC Website (www.nbcfdc.gov.in) and Loan & Employee Information Automation Project(LEAP) system which will be hosted at NIC Cloud Server.

The sealed bid should be submitted with superscription **"BID NO: NBCFDC/IT/WebSecurityAudit//2017 Dated: 27.09.2017"** on or before **23.10.2017** (**12:00 Hrs)** by hand or by post to :

AGM (Admn.) & CS
National Backward Classes Finance and Development Corporation
5th Floor, NCUI Building, 3, Siri Institutional Area,
August Kranti Marg, New Delhi-110016

3.   Important Dates

S.N.	Activity	Time Line
1	Issue of Tender	**27.09.2017**
3	Last Date & Time for Receipt of Bids	**23.10.2017 (12:00 Hrs)**
4	Date and Time for Opening of Technical/Commercial Bids	**23.10.2017 (15:00 Hrs)**

For any further announcement(s), please visit NBCFDC website i.e. **www.nbcfdc.gov.in**

4.   Scope Of Work

(1)   Name of the Application
   (i)   NBCFDC Website
   (ii)   Loan & Employee Information Automation Project(LEAP)

(2)   URL of Application with other main detail:
   (i)   Website – www.nbcfdc.gov.in

S.N.	Information about Website	Description
1	Web application Name & URL	http://nbcfdc.gov.in/
2	Operating system details	Linux (x86_64)
3	Application server with Version	Apache 2.2.31
4	Development platform for application : Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.)	PHP(5.4.45)
5	Whether the site contains any content management module	No
6	Back-end Database	MySQL(5.5.51-38.2)
7	No of input forms	Approx.(10)
8	No. (Approximate) of input Fields	Approx.(95)
9	No. of login modules	1
10	How many application roles/privilege levels of users	3
11	Does the application provide a file download feature	yes
12	Does the application provide a file upload feature	yes
13	Does the application has SMS integration	no
14	Does the application has E-Mail integration	no
15	Does the application has Payment Gateway integration	no
16	Static Pages	Approx.(68)
17	Dynamic Pages	Approx. (11)
18	Total Pages	79

(ii)   LEAP with other main detail - To be communicated (presently locally hosted)

S.N.	Information about Website	Description
1	Web application Name & URL	Not yet Hosted
2	Development Environment	Java 8, MySql 5.6, Eclipse Neon
3	Web Server	Apache Tomcat 7.5
4	Database server	MySql 5.6
5	Email integration Exist	Yes, in Recruitment Module
6	No of login Module	3
7	No of role	More than 5
8	No of dynamic Pages	More than 500
9	No of static Pages	Around 15

(3)   Selected bidder has to conduct application security assessment for all modules of the above mentioned applications. For conducting audit, the following minimum parameters are to be carried out:
   a.   Application Security Audit
   b.   Vulnerability Assessment
   c.   Penetration Testing

(4)   The audit shall also follow the Application Security Risks (as per OWASP Top 10 Application Security Risk), covering, but not limited to:
   a.   Injection
   b.   Cross-Site Scripting (XSS)
   c.   Broken Authentication and Session Management
   d.   Insecure Direct Object References
   e.   Cross-Site Request Forgery (CSRF)
   f.   Security Misconfiguration
   g.   Insecure Cryptographic Storage
   h.   Failure to Restrict URL Access
   i.   Insufficient Transport Layer Protection
   j.   Un-validated Redirects and Forwards

(5)   A full assessment comprising tests for all known web application vulnerabilities using both automated and manual tools based on the Open Web Application Security Project (OWASP) Testing Guide should be performed.

(6)   Compliance Review/Audit

   •   Based on above Audit report, the concerned developer shall make appropriate changes (rectifications) in the application. Upon intimation about completing such rectifications form the developers, the vendor will perform compliance check, to verify the rectification of all observations/recommendations prescribed

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

- All the activities under this audit should be carried out from NBCFDC office, New Delhi.
- As a part of the Audit, the agency shall follow the CERT-In guidelines regarding the security audit and shall cover the areas mandated by CERT-Ind. The auditors should rely heavily on technology, manual efforts & tools to perform the audit.

(7)   Deliverables

- Following deliverables are expected from the selected bidder for each application as specified in the scope of work:
- Submission of Draft Reports (First Testing Report) for Application Security Audit and Vulnerability Assessment
- Submission of Final Report after necessary round of testing and acceptance by the department for Application Security Audit and Vulnerability Assessment
- Both the audit reports should have details for corrective action and steps to remove identified vulnerabilities
- Agency should submit Compliance audit report. Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application has no vulnerabilities as a result of changes done in the code
- The final security audit certificate for should be in compliance with the NIC standards

(8)   Each Of The Above Mentioned Reports Shall Cover At Least The Following Areas:
1)   Executive Summary
2)   Background
3)   Scope of Work
4)   Approach & Methodology followed
5)   Overview of Work Done
6)   Detailed Findings and Recommendations:
   - Observation (classified in terms of Impact – Very High, High, Medium & Low)
   - Business Impact findings – Financial and Non-Financial
7)   Recommendations

5. **General Guidelines & Conditions:**

    a. <u>**Submission of Quote**</u>

    The quote must be submitted in sealed envelope with two bid system to ;

    AGM (Admn.) & CS
    National Backward Classes Finance and Development Corporation
    5th Floor, NCUI Building, 3, Siri Institutional Area
    August Kranti Marg, New Delhi-110016

    b. **Opening of Bids:**

    The quotes will be opened by constituted committee of NBCFDC. Vendor selection would be on the basis of best price quoted in proposal.

    c. Open/stapled/improperly sealed/received by fax/tenders received after stipulated time and day shall be treated as unresponsive.

6. **Prequalification of Quote**

    a. The firm should be registered with the Registrar of Companies/appropriate authority. Copies of PAN Number/Tan number/Sales/GST/Service tax number must be attached.

    b. The Bidder must have done at least one security audit of website/application implementation in Govt. Departments/ PSUs.

    c. The Bidder must be empanelled with **Cert-In**.

    d. The firm should not have been blacklisted by any Government Department in India. (Please attach an undertaking signed by the authorized representative of the Agency)

7. **Tender Fees**

Tender document may be downloaded from the website www.nbcfdc.gov.in A demand draft of Rs.500/- (Rupees Five Hundred only) from any commercial bank drawn in favor of "**National Backward Classes Finance and Development Corporation**, 5th Floor, NCUI Building, 3, Siri Institutional Area, August Kranti Marg, New Delhi-110016" payable at New Delhi shall be submitted along with the bid and it is non-refundable.

The bidders registered with NSIC, are exempted for payment of tender fee, if they produce a valid certificate.

8.   Payment Terms

      a.   Payment will be released only after submitting the final security audit certificate.

9.   Earnest Money Deposit

Bidders have to submit EMD(interest free) of Rs. 5,000/- which will be refunded:

      a.   To Unsuccessful bidders after acceptance of contract by successful bidder

      b.   To Successful bidder after submission of security audit certificate to NBCFDC.

      c.   The bidders registered with NSIC, are exempted for payment of EMD, if they produce a valid certificate.

      EMD submitted by the bidder will be forfeited if:

      a)   The bidder withdraws or amends its tender or derogates from the tender in any respect within the period of validity of its tender. Further, if successful tenderer after receiving the LoA, fails to submit the security audit certificates, EMD will be forfeited

      b)   The bidder withdraws his bid after processing but before acceptance of award of contract issued by NBCFDC

      c)   The bidder violates any of the provisions of the terms and conditions of the tender specifications

      d)   Final decision on EMD forfeiture will rest with the Competent Authority of NBCFDC

10.   Authorized Signatory

The selected bidder shall indicate the authorized signatories who can discuss and correspond with NBCFDC, with regard to the obligations under the contract.. The bidder shall furnish proof of signature identification for above purposes as required by NBCFDC

11.   Other Terms and Conditions

      a.   Non-transferable Offer;

      This Offer document is not transferable. Only the party, who has purchased this offer document, is entitled to quote.

      b.   Only one Proposal;
      The Bidder should submit only one proposal. If the Bidder submits or participates in more than one proposal, such proposals shall be disqualified

      c.   Validity of Offer;
      The offer should be valid for a minimum period of 90 days from the date of submission. The Bids valid for a period shorter than specified period shall be rejected.

d. Clarification and amendment in Tender ;
Clarification at any time before/upto 10.10.1027. Further, NBCFDC may amend the tender document by issuing an addendum/corrigendum upto 16.10.2017, if required.

e. **The website and LEAP software will be hosted at NIC server after Security audit, so the Security Audit Certificate should be in compliance with the NIC standards.**

f. Tender Fee and EMD(interest free) be submitted along with Technical Bid.

g. Each and every page of the bid document be signed by the authorised person

h. Identification and prioritization of various risks to the web application

i. The first round of security audit report should be submitted to NBCFDC within 10 days after the job order issued by NBCFDC and consecutive round report if any, should be submitted within 5 working days.

j. The contract with the selected bidder shall be governed in accordance with the Laws of India and will be subject to the exclusive jurisdiction of Courts at Delhi (with the exclusion of all other Courts)

Prescribed Format for Technical Quote (Compulsory)

S.N.	Criteria	Whether minimum Eligibility criteria fulfilled (Yes/No)	Details of Supporting documents attached. (Page No.)
1	The firm should be registered with the Registrar of Companies/appropriate authority. Copies of PAN Number/Tan number/Sales/GST/Service tax number must be attached		
2	The Bidder must have done at least one security audit of website/application implementation in Govt Departments/ PSUs.		
3	Copy of authorization with CERT-in empanelment		
4	The Agency should not have been blacklisted (Please attach an undertaking signed by the authorized representative of the Agency).		
5	The firm should have its office in New Delhi/NCR.		
6	Tender Fee(non-refundable) of Rs. 500/-(Rupees Five Hundred only) and EMD (refundable) of Rs. 5,000/-(Rupees Five Thousand only) in the form of Pay Order/Demand Draft/Bankers' Cheque in favour of NBCFDC payable at New Delhi.		
7	The enclosed certificates and documents should be self-attested by the Agencies.		

Prescribed Format for Financial Quote (Compulsory)

Financial Bid	
Financial Bid For (Name of Tender)	
Company Name	
Address	
Pin Code	
Telephone No.	
Email Id	
Contact Person Name	

S.No.	Description of Service	Amount(Rs.)	Remarks
1	Security Audit certificate along with report and assessment via tool etc.		
Tax on above service component			
Total Charges			

Name of authorized signatory: Signature and Company Seal

(To be furnished on the Bidder company's Letter-Head)

Undertaking for Non Black-listing

Certified that We M/s_____ have not been, blacklisted by any Government Department / organizations, on account of defective /deficient services provided by us or any reason related to the Business Practices.