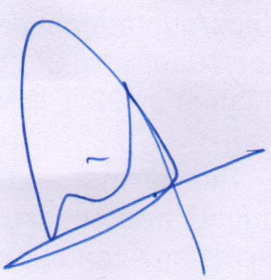
File No. C-12020/1/2021-CC (Limited Tender Enquiry)

Note:- Only Delhi/ NCR based CERT-In Empanelled Information Security Auditing Organizations as per list available at https://www.cert-in.org.in/PDF/Empanel_org_2022.pdf are authorized to participate in bid. Any other bid, by other than these CERT-In Information Security Auditing Organizations, will be summarily rejected.



राष्ट्रीय मानव अधिकार आयोग
National Human Rights Commission
Manav Adhikar Bhawan, C-Block, GPO Complex,
INA, New Delhi–110023 INDIA
Fax : 91-011-24651329
E-mail : nhrcga@nic.in
Website : www.nhrc.nic.in

eFile No.C-12020/1/2021-CC Dated : 06TH JUNE, 2024

Last Date For Submission of Tender is 28TH JUNE, 2024 upto 5 PM

NOTICE INVITING TENDER (Limited Tender Enquiry)
FOR AWARDING CONTRACT FOR SECURITY AUDIT OF THE HRCNET PORTAL

The National Human Rights Commission is interested to award Contract for Security Audit of the HRCNet Portal (https://hrcnet.nic.in) of the Commission.

Any inquiry regarding aforesaid matter can be made from Sr. System Analyst (Telephone No. 24663228) on any working day between 10:30 AM to 04:00 PM.

1. TENDER

(i) The interested parties may submit their bids/quotations (in the form of **two bid** system viz. Technical Bid and Financial Bid) in a sealed envelope superscribed in Bold Letters as **"Quotation for** Annual contract for Security Audit of the HRCNet Portal" and addressed to the Under Secretary (G.A.), National Human Rights Commission, Manav Adhikar Bhawan, Block – C, G.P.O. Complex, INA, New Delhi-110023. The bids/quotations accompanied must be dropped in the Tender Box placed in C.R. Section (Room No.04) at Manav Adhikar Bhawan, Block – C, G.P.O. Complex, INA, New Delhi latest by **28TH JUNE, 2024** as per the instructions given in this tender notice.

(ii) The terms and conditions, which are given below, may be gone through thoroughly and ensure to make a specific mention in your quotation to that effect that the terms and conditions are acceptable to you, in full.

(iii) The tenderers are expected to examine all the instructions, terms and conditions and specifications in the tender documents. Failing to furnish all information required by the tender document in every respect will be at the tenderer's risk and may result in rejection of the tender/bid.

2. BIDS

2.1 TECHNICAL BID – This bid shall contain the following documents (All Essential):-

(i) DECLARATION - The Declaration (**Annexure – I**) duly filled up and signed by the authorised signatory of the bidding firm should be kept in **Technical Bid** envelope alongwith other documents/ information prescribed in this tender notice;

(ii) REGISTRATION CERTIFICATE - The bidder must furnish a copy of the Registration Certificate of the firm;

(iii) EXPERIENCE & LIST OF CLIENTS - The bidder must have at least 02 years experience in the field and furnish list of clients in Govt./Semi Govt. Sectors/PSUs with address, name of contact person and contact numbers where they have similar contracts and also submit the certified copies of contracts of at least 02 organizations;

(iv) UNDERTAKING ABOUT BLACKLISTING - The bidding firm should not have been **blacklisted** by any Government/ Semi-Govt Department. The bidder should furnish an **Undertaking** to this effect (in **Annexure-I**) that they (firm/agency) have not been blacklisted by Govt/Semi Department/office;

(v) GST/ PAN - The bidder must have GST and PAN number. The Copies of the GST certificates/ PAN Card should be enclosed as a proof;

(vi) **Bid Security Declaration**- In place of a Bid security/EMD, the bidders has to accept /sign the **Bid Security Declaration**; and

(vii) **Cert-in Empanelment Certificate** - The bidder must have latest valid certificate of Cert-in empanelment. Copy of certificate should be enclosed as proof.

(viii) **Geographically presence** - The bidder must have at least 01 Technical Operational Office in Delhi/ NCR.

2.2 FINANCIAL BID – This Bid shall contain the rate quoted by the bidder:-

(i) FINANCIAL BID - The bidder shall quote/indicate the rates for all items (in Indian Rupees) offered by it in the *'Proforma for Financial Bid'*, placed at **Annexure – II**. Please quote rates in appropriate column;

(ii) The bidder must quote the price excluding/without GST/Service Tax.

2.3 GENERAL INSTRUCTIONS:-

(i) The technical bid and the financial bid should be sealed by the bidder in separate covers duly superscribed and both these sealed covers are to be put in a bigger cover which should also be sealed and duly superscribed in bold letters as "Quotation for Annual contract for Security Audit of the HRCNet Portal";

(ii) The technical bids would be opened in the first instance and evaluated by a committee and only the technically acceptable bids would be considered further;

(iii) The bids received after due/last date and time will not be accepted; and

(iv) The quotations / bids which are not in conformity with the instructions contained in the NIT are liable to be rejected. However, in any case, the Commission reserves the rights to reject any bid/quotation without assigning any reasons.

3. SCOPE OF WORK:

Bidder would be expected to perform the tasks for the web application security to analyze and review the web application. The auditors will have to carry out an assessment of the vulnerabilities, threat and risks that exist in web application through Internet Vulnerability Assessment and Penetration Testing etc. This will include identifying remedial solutions and recommendations for implementation of the same to mitigate all identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security of the web application. The bidder will also be expected to propose a risk mitigation strategy as well as give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment. The Web application should be audited as per the Industry Standards, Cert-in guidelines, NIC guidelines and also as per the OWASP (Open Web Application Security Project) model. The auditor is expected to submit the final audit report after the remedies / recommendations are implemented. The final report will certify the particular web application as "Certified for security, safe for hosting and secured for deployment". All the web application security audit reports should contain the details as mentioned at the Audit report.

The scope of the proposed audit tasks is given below. The audit firm / company will be required to prepare the checklist / reports.

Details of web application:-

URL of the app	https://hrcnet.nic.in
No of dynamic pages	around 600
No of static Pages	around 50
No. of login modules	10
No of roles	17
software environment of the application	Windows Server 2012/2016, ASP .Net, Java Script, Bootstrap
Database	SQL server 2012

Task 1: Web Application Security Audit / Assessment

The various check / 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
- HTTP Injection
- Phishing a website
- Buffer Overflows, Invalid inputs, insecure storage etc.
- Other any attacks, which are vulnerability to the website and web applications.
- The Top 10 Web application vulnerabilities, which are given below, should alsochecked from the given websites:

A1 – Cross Site Scripting(XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attacks to execute script in the victim's browser which can hijacks user sessions, deface web sites, possibly introduceworms, etc.
A2 – Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 – Malicious FileExecution	Code vulnerable to remote file inclusion (RFI) allowsattackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework, which accepts filename or file from users.
A4 – Insecure Direct Object Reference	A direct object reference occurs when a developerexposes a reference to an internal implementation object, such as a file, directory, database record, or key as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 – Cross Site RequestForgery (CSRF)	A CSRF attack forces a logged- on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be powerful as the web application that it attacks.
A6 – Information Leakageand Improper Error Handling	Application can unintentionally leak information about their configuration, internal working, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attack.
A7 – Broken Authentication	Account credentials and session tokens are often not protected. Attackers compromise passwords, keys or authentication tokens to assume other users' identities.
A8 – Insecure Cryptographic Storage	Web application rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 – Insecure Communication	Applications frequently fail to encrypt network traffic whenit is necessary to protect sensitive communication.
A10 – Failure to RestrictURL Access	Frequently an application only protects sensitive functionality by preventing the display of links or URLs to unauthorised users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

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

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

If vulnerabilities are observed from the re-audit, the vendor must provide a detailed recommendations report on the vulnerabilities observed or found from Re-audit / Task2. The audit firm / company must submit a summary compliance report at end of each task and the final report should certify that the website/ web applications (should mention the name of website and/or web application) is "Certified for security, safe for hosting and secured for deployment."

1. Deliverables and Audit Reports

(a) The successful bidder will be required to submit the following documents after the audit for Web Application, as mentioned below and the audit firm must also submit suggestions / recommendations and other detailed steps for enhancing the website security

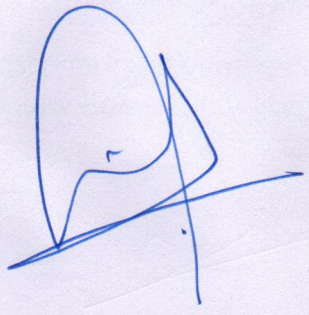
(i) A detail report will be submitted with security status and discovered vulnerabilities, weaknesses and mis-configurations with associated risk levels and recommendedactions for risk mitigations.

(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

(iii) All deliverables shall be in English language and A4 size format and through e-mail.

(iv) The vendor will be required to submit the deliverables as per agreed implementation Plan

□ The deliverables (like Audit Certificate, 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 mentionedin the Task1 and Task2



(b) Audit Report and certificate

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

1. Identification of auditee (Address & contact information)

2. Dates and Location(s) of audit

3. Terms of reference (as agreed between the auditee and auditor), including thestandard for Audit, if any

4. Audit plan

5. Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents

6. Additional mandatory or voluntary standards or regulations applicable to the auditee

7. Standards followed

8. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)

a. Tools used
b. List of vulnerabilities identified.
c. Description of vulnerability
d. Risk rating or severity of vulnerability
e. Test cases used for assessing the vulnerabilities
f. Illustration if the test cases to provide the vulnerability
g. Applicable screen dumps

9. Analysis of vulnerabilities and issues of concern

10. Recommendations for action

11. Personnel involved in the audit, including identification of any trainees

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

4. TERMS & CONDITIONS:

(i) The contract shall be awarded for a period of 02 months/60days from the date of commencement of the contract. However, the Commission reserves the right to terminate the contract giving one month's notice without assigning any reasons or to entrust the job to any other firm / party at the risk / expenses of the defaulting contractor;

(ii) The rates once quoted by the vendor will remain valid throughout the contract period;

(iii) In place of a Bid security, the Bidders has to accept /sign the **"Bid Security Declaration"**;

(iv) The contract charges/ payment will be released after completion of work;

(v) The Commission shall deduct TDS u/s 194c of the IT Act, 1961 & GST respectively

(vi) The contracted firm shall invariably furnish the complete address of the premises of its offices, go-downs and workshops where inspection can be done together with full name & address of the person who is to be contacted for this purpose;

(vii) Hypothetical or conditional tenders will not be entertained. Tender once submitted shall not be allowed to be withdrawn or altered. If the tender is withdrawn or altered by the concerned party at any time after it is submitted, appropriate action may be taken;

(viii) Over-writing/over-typing or erasing of the figures which render it doubtful or ambiguous are not allowed and shall render the tender invalid;

(ix) The Commission shall have no liability, financial or otherwise, for any harm/damage/injury incurred by the manpower deployed by the contractor in the course of performing the work in the Commission or at any other place. **Neither the tenderer nor his engineers/workers shall have any claim on this Commission for compensation or financial assistance on this account.**

Major Vishnu SP
Under Secretary (GA)

Enclosed: Annexure-I & II

Annexure - I

DECLARATION

(To be kept in Technical Bid Envelope)

M/s _____

(Name, address and Landline and Mobile No. of bidding the bidding firm/agency):-

S. No.	Documents kept in the 'Technical Bid' envelope	Whether enclosed (The firm would write YES or NO)	Page No.
01	Copy of Registration/License of the firm		
02	Certificate/proof/documents regarding at least 02 year experience in the field		
03	Experience – List of Clients Govt/Semi Govt./ PSUs offices with address, name of contact person and contact numbers and certified copies of AMC/ contracts of at least 02 organizations.		
04	Self certificate in respect of not being blacklisted from any Government Ministry/Department		
05	GST registration certificate of the contractor/ agency / firm.		
06	Copy of PAN.		
07	Bid Security Declaration		
08	Cert-in Empanelment Certificate		
09	Geographically presence - The bidder must have at least 01 Technical Operational Office in Delhi/ NCR.		

i) It is hereby declared that the Terms & Conditions of the NHRC's NIT No.C-12020/1/2021-CC dated 6th JUNE, 2024 are **fully acceptable to this Firm / Agency.**

ii) It is also declared that our firm has **never been black-listed** by any government/Semi Govt department.

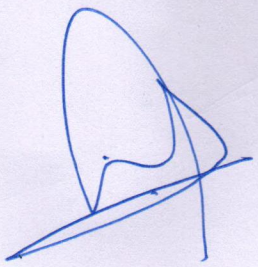
iii) "Bid Security Declaration"

(a) That I / we have availed the benefit of waiver of EMD while submitting our offer against the subject Tender and no EMD being deposited for the said tender.

(b) That in the event we withdraw or modify our bid during the period of validity Or I/we have awarded the contract and I/we fail to sign the contract Or to submit a performance security within given time line and I/we will be suspended from being eligible for bidding/ award of all future contract(s) of National Human Rights Commission for a period **of two years** from the date of committing such breach.

(To be signed by the Authorized Signatory
of the Firm/Agency with Name and Stamp)

Note:-Financial bids of only those firms will be opened who qualify in the technical bids.



Annexure – II

FORMAT FOR FINANCIAL BID

(for quoting rates in Indian Rupees)

Name & Address of Firm : -
(With Telephone No. & Mobile No.)

_____

_____

_____

Contract for Security Audit of the HRCNet Portal

S.No.	Rates Quoted (in Rs.) excluding taxes
1.	

(To be signed by the Authorised Signatory
of the Firm/Agency with Name and Stamp)