ज्ञान-विज्ञान विमुक्तये

शैक्षिक संचार संकाय

**Consortium for Educational Communication**

(An Inter University Centre of University Grants Commission on Electronic Media)
IUAC Campus, Aruna Asaf Ali Marg, New Delhi-110067 (INDIA)
Phone : +91-11-24126418-19-20 Fax : +91-11-24126416
Website : www.cec.nic.in, E-mail : info.cec@nic.in

**F.No.CEC/Multimedia/SA & VA-NIC/2023**/816948 **Dt : 03.11.2023**

**To,**

**As per List**

**Subject:- IT Security Audit - Calling of Quotations reg.**

Dear Sir/Madam,

The Consortium for Educational Communication (CEC), New Delhi hereby invites Sealed Quotation from interested and eligible NICSI or CERT-In enlisted companies/firms/agencies for Web Security Audit, who have prior experience of handling Security Audit for Govt. Organizations (copy of the order of the organization to be enclosed for authentication).

1. CEC (Consortium for Educational Communication) desires to get routine Security Audit done for its
    a. Website
    b. Web Based Library Management System

    Both hosted at webservers located at NIC Data Centre, Shastri Park, New Delhi

2. An Earnest Money Deposit (EMD) of Rs. **1500**/- (Rupees One Thousand Five Hundred Only) in the form of Demand Draft/Pay Order in favour of Director, CEC payable at New Delhi should be enclosed with the quotation in a sealed envelope subscribed 'Quotation for IT Security Audit'.

3. Sealed quotation should be addressed to the **Chief Administrative Officer, Consortium for Educational Communication, IUAC Campus, ArunaAsaf Ali Marg, New Delhi – 110067**. The quotation may be sent by Hand/Speed/Registered Post to the above mentioned address or may be dropped in the tender box placed at CEC, New Delhi at above address latest by 28th Nov 2023. upto 02:30 PM. The tender will be opened on the same date at 03:00 PM.

4. The tenderer should quote for all the columns/ items in Financial Bid as per **Annexure-'A'**, failing which the bid shall be considered non-responsive, incomplete and tender will be summarily rejected.

5. The copy of the scope of work for the Security Audit is enclosed.

6. In case the successful Tenderer declines the offer of Contract, for whatsoever reason(s), his EMD will be forfeited.

7. The EMD will be refunded to the unsuccessful tenderer only after finalization of the contract. No interest is payable on the EMD.

8. Each page of the Tender Document and papers submitted along with, should be serially numbered, signed and stamped by the authorized signatory.

9. All entries in the Tender form should be legible and filled clearly. Any overwriting or correction which is unavoidable has to be signed by the authorized signatory.

10.The vendor must have successfully completed minimum two Security Audits in CPSUS/Govt. Organisations / Leading Commercial Organisations during the last 3 years.

11. Vendor must have a support office located in Delhi/NCR with a help desk facility in their office.

12. The tender will be valid for 90 days.

13. CEC reserves the right to reject the tender without assigning any reason thereof.

14. The time limit for IT Security Audit completion will be 3 weeks effective from the date of work order.

15. In Financial Bid, wherever options are given, cost of Security Audit and taxes, if any be given separately in the prescribed format, otherwise the bid is liable to be rejected.

16. The payment will be made through Cheque/NEFT after successful IT Security Audit and submission of audit certificate.

Yours faithfully,

(Navin Soi)
Chief Administrative Officer

Encl. As above

Annexure-A

## FINANCIAL BID

| S.No | Particulars | Cost<br>(In Rupees) |
|---|---|---|
| 1 | Cost of Security Audit<br>a. CEC Website<br>b. Web based Library Management System | |
| 2. | GST (if applicable) | |
| 3. | Any other taxes (if applicable) | |
| | **TOTAL COST** | |

Signature of the Tenderer

Name of the Tenderer

Address & Seal

Telephone No.

# Scope of Work for the Security Audit for CEC Website and Web Based Library Management System

## A. CEC Website

The website has been developed in-house by CEC and is running successfully on CEC webservers located at NIC Data Centre, Shastri park, New Delhi. Basic information of CEC website is mentioned below. The website consists of approx 1000 numbers of static/dynamic pages.

| S.No. | Parameters | Description |
|---|---|---|
| 1. | Web Application Name & URL | cec.nic.in |
| 2. | Operating System Details<br>(E.g. Windows-2003, Linux, AIX, Solaris, etc.) | Microsoft windows datacenter 2019 (64bit) |
| 3. | Application Server with Version<br>(E.g. IIS 5.0.Apache, Tomcat, etc. ) | Apache |
| 4. | Front-end Tool [Server side Scripts]<br>(E.g. ASP, Asp.NET, JSP, PHP, etc.) | PHP |
| 5 | Back-end Database<br>(E.g. MS-SQL Server, PostgreSQL, Oracle, etc. ) | MySQL |
| 6. | Authorization No. of roles & types of privileges for the different roles | 2 |
| 7. | Whether the application contains any content management System (CMS) (If yes then which?<br>(E.g. Joomla/WordPress/Drupal/Liferay etc.) | Yes, Drupal 7 |
| 8. | Total No. ( Approximate) of Input Forms | 2 |
| 9. | Total No. of input fields | 1 |
| 10. | No. of login modules | 2 |
| 11. | Whether the application is to be audited for Application Security Vulnerabilities for the 1st time? | NO |
| 12. | Any other information, you would like to provide. | Used CMF (Content Management Framework) developed by NIC. NIC developed CMF, using Drupal 7. |

## B. Web Based Library Management System

Web Based Library Management System developed in-house by CEC is successfully running since 2017 on server located at NIC Data Centre. CEC has recently replaced the old servers with new servers. Hence the application has to be audited again before installing on the new server. The basic information of Web based Library Management system is mentioned below:

| S.No. | Parameters | Description |
|---|---|---|
| 1. | Web Application Name & URL | cecmedialibrary.nic.in, Web Based Library Management System |
| 2. | Operating System Details<br>(E.g. Windows-2003, Linux, AIX, Solaris, etc.) | Microsoft windows datacenter 2019 (64bit) |
| 3. | Application Server with Version<br>(E.g. IIS 5.0.Apache, Tomcat, etc. ) | IIS |
| 4. | Front-end Tool [Server side Scripts]<br>(E.g. ASP, Asp.NET, JSP, PHP, etc.) | Asp.NET |
| 5 | Back-end Database<br>(E.g. MS-SQL Server, PostgreSQL, Oracle, etc. ) | SQL Server 2019 |
| 6. | Authorization No. of roles & types of privileges for the different roles | 7(MCD,PRE,REC,MCDE,MCP,LADMIN,JD) |
| 7. | Whether the application contains any content management System (CMS) (If yes then which?<br>(E.g. Joomla/WordPress/Drupal/Liferay etc.) | No |
| 8. | Total No. (Approximate) of Input Forms | 1 |
| 9. | Total No. of input fields | 30 |
| 10. | No. of login modules | 275 |
| 11. | Whether the application is to be audited for Application Security Vulnerabilities for the 1st time? | NO<br>Application successfully running since 2017 on server located at NIC Data Centre, Shastri Park, New Delhi |
| 12. | Any other information, you would like to provide. | |

## Scope of Work

1. The Auditor is expected to carry out an assessment of the vulnerabilities, threats and risks that may exist in the above application/website through Internet Vulnerability Assessment and Penetration Testing which includes identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security.

2. The audit should be done by using Industry Standards and as per the Open Web Application Security Project (OWASP) methodology.

3. During Security Audit, if any lapse is found, the same shall be reported by the auditor to CEC for making the application/website fully secured for hosting on NIC server.

4. The Audit should be conducted in conformity with NIC audit guidelines. After successful security Audit, the security audit report from the auditor should clearly state that all web pages along with respective linked data files (in pdf / doc / xls etc. formats), all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website/application.

5. **Responsibilities of Selected Auditor:**

   The Selected Auditor will conduct security Audit for the CEC as under:

   5.1. Verify possible vulnerable services, only with explicit written permission from the auditee.
   5.2. Notify the auditee whenever there is any change in auditing plan / source test venue / high risk findings or any occurrence of testing problem.
   5.3. Responsible for documentation and reporting requirements for the audit.
   5.4. Task-1: Web Security Audit/Assessment.
   5.5. Task-2: Audit based on recommendation report of Task-1.
   5.6. On successful security audit, furnish certificate for the Website / Web based Library Management system as per NIC norms stating that the Website / Web based Library Management system is safe for hosting on the NIC server.

6. **Audit report**
   The Auditor shall submit a report indicating about the vulnerabilities as per OWASP and recommendations for action after completion of Task-1. The final formal IT security Audit Report should be submitted by the Auditor after the completion of all the tasks of Audit. The reports should contain:
   6.1. Identification of auditee (address & contact information).
   6.2. Dates and locations(s) of audit (Task-1 and Task-2)
   6.3. Terms of reference (as agreed between the auditee and auditor), including the standard for audit, if any.

6.4. Audit Plan.

6.5. Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents, if any.

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

6.7. Summary of audit findings including identification tests, tools used and results of tests performed.

6.8. Analysis of vulnerabilities and issues of concern.

6.9. Recommendations for action.

6.10. Personnel involved in the audit, including identification of any trainees. In addition to this, reports should include all unknowns clearly marked as unknowns.

7. **Confidentiality**

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

**Deliverables and Audit Reports:**

The successful bidder will be required to submit the following documents in printed format (2 copies each). After the audit of above mentioned web application:

i. A detailed report with security status and discovered vulnerabilities weakness and misconfigurations with associated risk levels and recommended actions for risk mitigations.

ii. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by CEC.

iii. The final security audit certificate for and should be in compliance with the NIC standards.

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

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

**Duration / Completion of Contract:** Three weeks from the date of award of the contract.