Request for Proposal

Scope of Work

1. Primary objective of the Security Audit is to identify major vulnerabilities in the Website from internal and external threats.
2. Security Audit should be done using Industry Standards and as per latest Open Web Application Security Project (OWASP) guidelines / methodology including but not limited to the following :
    a) 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, HTTP injection, Phishing a website, Source code manipulation, Buffer Overflows, Invalid Inputs, Insecure Storage etc.
    b) Identify the security vulnerabilities including top web application vulnerabilities viz Cross Site Scripting (XSS), Injection Flaws, Malicious File Execution, Form / Hidden field manipulation, Command injection, Insecure Direct Object Reference, Cross Site Request Forgery (CSRF), Information leakage and Improper Error Handling, Broken Authentication and Session Management, insecure Cryptographic Storage, Insecure Communications, Failure to Restrict URL Access, Etc.
    c) The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist web application through Internet Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementations of the same to mitigate all identified risks, with the objective of enhancing the security of the system.
    d) Undertake user profiling and suggest specific access methodologies and privileges for each category of the users identified.
    e) Any other attacks, to which the Website could be vulnerable.
    f) Identification and prioritization of various risks to the website.
    g) must adhere to Cert-in Guidelines.
    h) Identify remedial solutions and recommendations for making the web application secure.
3. The auditor shall also carry out "Black Box Testing" of the Website.
4. NIELIT shall not provide any tools that may be required for the said purpose.
5. As the website is already hosted and live on NIC servers, the auditor shall carry out security remedies.
6. Once the threats are identified and reported, the auditor shall also suggest possible remedies.
7. The auditor shall share final detailed review report and recommendations along with solutions.
8. The auditor shall conduct Post Security Audit after implementing the recommendations.
9. The auditor will coordinate with NIELIT to fix the vulnerabilities found during the Security Audit till all issues are fixed irrespective of number of iterations and till audit clearance certificate is issued.

10. The auditor will provide support to resolve any issue, if raised by NIC before accepting the audit Certificate, in co ordination with NIELIT.

Terms and Conditions

1. Bidder submitting the quotation should be CERT-in empanelled "Information Security Audit organization". The bidder shall enclose a copy of the valid empanelment certificate. Bid without empanelment certificate shall not be considered.
2. The selected agency will not outsource any activity to other agency.
3. The selected agency shall maintain confidentiality of the finding of security audit and ensure that findings and corrective actions are shared with NIELIT and its AMC team only.
4. NIELIT shall not make any additional payment of any sort for usage of any tools / software etc for conducting the Security Audit of the website.
5. The Security Audit of the website shall be completed within 15 days from the date of issue of the order excluding the days taken to fix the vulnerabilities by AMC team. However, NIELIT may at any time terminate / cancel the work order, if the agency is unable to provide the services as per the work order. No payment will be made to the agency, in that case.
6. If the agency with whom the work has been assigned backs out the agency shall be liable to pay the difference of amount, which this office may have to incur at higher rates vis-a-vis those contracted with it, through alternative means. Further the act of backing out will automatically debar the agency for any further consideration for any work by this office.
7. The prices quoted should be net and all inclusive. Rates of taxes etc if separate should be clearly specified.
8. Quotation Validity: At least three months form the closing date.
9. Payment terms: 100 % after clearance from NIC. No advance payment will be given by NIELIT.
10. The quotations should be properly sealed. Quotations through fax / Email shall not be accepted.
11. Sealed quotation shall reach following address before due date:
    "The director, NIELIT, 2nd floor, Parsvanatha metro mall, Inderlok Metro station, Dehi-110052".
12. The quotation received after due date will be rejected.
13. Mark the envelop "Security Audit of NCPSL Website: Due Date June 7, 2018 ".
14. Incomplete or conditional quotation will not be entertained
15. The printed conditions on your quotations, if any, shall not be binding on us.
16. The bidder shall attach a signed and stamped copy of this letter marking "All terms and conditions are accepted ".

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 of national Council for Promotion of Sindhi Language, Govt of India (NCPSL):

1. A detailed report with security status and discovered vulnerabilities weakness and mis-configurations with associated risk levels and recommended actions for risk mitigations.
2. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by NIELIT.
3. The final security audit certificate should be in compliance with the NIC standards.
4. All deliverables shall be in English language and in A4 size format as prescribed by CERT-IN.
5. The vendor will be required to submit the deliverables as per terms and conditions of this document.

Information about the Application

S. No	Parameters	Description
1.	Web Application Name & URL	NCPSL
2.	Operating System Details (E.g. Windows-2003, Linux, AIX, Solaris, etc.)	LINUX
3.	Application Server with Version (E.g. IIS 5.0. Apache, Tomcat, etc.)	Apache Tomcat 9.0
4.	Front-end Tool [Server side Scripts] (E.g. ASP, Asp.NET, JSP, PHP, etc.)	JSP and Servlets
5.	Back-end Database (E.g. MS-SQL Server, PostgreSQL, Oracle, etc.)	MySQL 5.7
6.	Authorization No. of roles & types of privileges for the different roles	1 - Admin
7.	Whether the application contains any content management System (CMS) (If yes then which? (E.g. Joomla/WordPress/Drupal/Liferay etc.)	No
8.	Total No. (Approximate) of Input Forms	35 approx.
9.	Total No. of input fields	500*(approx.)
10.	No. of login modules	1
11.	How many pages(in total) static/ Dynamic are there in the application	20
12.	Lines of Code in the application	3500
13.	Number of Web Services, if any	N/A
14.	Payment Gateway, if any	N/A
15.	Online Testing Possible	Yes
16.	Whether the application is also hosted in the staging environment	Yes
17.	Whether the testing can be done off-site?(either over VPN connectivity or netting the staging server to internet)	Yes
18.	Does the application provide a file download feature (Yes/No)	Yes
19.	Does the application use Client side certificate (Yes/No)	No
20.	Tentative Testing environment (Development / Staging/	Staging

	Production Box)?	
21.	Does the application has SMS integration (Yes/No)	No
22.	Does the application has E-mail integration (Yes/No)	No
23.	Does the application provide a file upload feature(Yes/No)	Yes

*Number of Input field depends upon manageable contents in the website.