No. 10/2/2018-OIDB Dated: 12-04-2023

Invitation of Bids for Security Audit of OIDB's website at OIDB Bhawan, Sector-73 Noida

Oil Industry Development Board (OIDB) invites bids from NICSI/NIC empanelled agencies having experience in Security Audit of websites for Security Audit of OIDB's Website bilingual i.e. www.oidb.gov.in		
Sl. No.	**Item**	**Description**
1.	Scope of Work	Security Audit of OIDB's bilingual website (www.oidb.gov.in) in compliance to the Guidelines for Indian Government Websites and clearance of patches with vulnerabilities score of 80% and above
2.	Type of bid	Two bid system: (1) Technical Bid (2) Financial Bid Both the bids to be submitted separately online on GeM Portal
3.	Availability of Bid document on	GeM Portal OIDB's Website –www.oidb.gov.in
4.	Submission of Bid document on	GeM Portal
5.	Earnest Money Deposit (**E**MD)to be submitted with the tender document	3% of the contract value through NEFT/RTGS in favour of OIL INDUSTRY DEVELOPMENT BOARD **A/C No. 11084240909** State Bank of India, Main Branch, Parliament Street, New Delhi. **IFSC: SBIN0000691**
6.	Tender upload date and time	12-04-2023 (As per Gem)
7.	Last date and time of submission of bids	23-4-2023 at 5.00 pm
8.	Date of opening of Technical bid	24-4-2023 at 11.00 am
9.	Estimated cost of the contract	Rs. 1.80 Lakhs (inclusive of GST)
10.	Period of contract	One (01) month
11.	Contact person	Shri Sanjay Kashyap, Manager (P&A)
2	**PREQUALIFICATION CRITERIA (PQC)**	
2.1	The bidder should be empanelled with NICSI/NIC as on date of submission of bid- copy of empanelment letter to be submitted.	
2.2	Bidder should have its registered/branch office at Delhi/NCR.	
2.3	Bidder should have valid PAN and GST registration.	
2.4	Bidder should have an average annual financial turnover of at least **30%** of estimated cost of contract during last 3 years, ending 31 March 2022.	

2.5	Bidder should have during last 3 years ending 31st March, 2022 successfully completed any of the following works in CPUs/State PSU/Central or State Govt./Semi Govt.: Three similar completed works costing not less than the amount equal to 40% of the estimated cost of contract **OR** Two similar completed works costing not less than the amount equal to 50% of the estimated cost of contract **OR** One similar completed work costing not less than the amount equal to 80% of estimated cost of contract Copy of completion certificate to be submitted. Similar work means experience in Security Audit of website.
2.6	Similar work means experience in Security Audit of website. The bidder should have performed at least 2 nos. of Website Security Audits in Govt. sector- Copy of certificate to be attached.
2.7	Offer of bidder who is under liquidation and/ or whose net worth going negative will not be considered. A declaration/undertaking to this effect shall be submitted mandatorily by the bidder. Audited Balance Sheet of latest financial year has to be submitted.
2.8	Bidder should not be holiday listed/black listed by OIDB or any of Govt./PSU. A declaration/undertaking to this effect shall be submitted mandatorily by the bidder.
2.9	Documentary proof in respect of prequalification criteria should be submitted with technical bid as per **Annexure – I.** OIDB reserves the right to complete the evaluation based on the details furnished without seeking any additional information.

Annexure I

Sl. No.			**To be filled by the bidder and documents to be attached.**
1		Address of Registered/branch office at Delhi/NCR	
2.	i	PAN No.	
	ii)	GST registration number	
3.		**Annual turnover of the bidder (Audited Balance Sheet to be submitted)**	
	i	2019-20	
	ii	2020-21	
	iii	2021-22	
4.		**Experience of having successfully completed similar work in CPUs/State PSU/Central or State Govt./Semi Govt. during last 3 years ending 31st March, 2022**should be either of the following : Three similar completed works costing not less than the amount equal to 40% of the estimated cost of contract **OR** Two similar completed works costing not less than the amount equal to 50% of the estimated cost of contract **OR** One similar completed work costing not less than the amount equal to 80% of estimated cost of contract	
	i.	Name of the organisation	
	ii.	Annual value of the contract inclusive of taxes	
	iii.	Years of contract	
	iv.	Completion Certificate of the work	
5.		A declaration/undertaking to this effect that bidder is neither under liquidation nor is bidder's net worth going negative.	
6.		A declaration/undertaking to this effect that Bidder is not be on holiday listed/black listed by OIDB or any of Govt./PSU.	
Note:			
1. Above information to be furnished with supporting documents.			
2. Annexure-I not filled with desired information & supporting documents may invite disqualification.			
3. Additional sheet may be used in case of insufficient space.			
4. Bidder, contractor, vendor, service provider or agency referred to in this NIT and /or any document presently and/or subsequently related thereto shall first mean the bidder and contractor after award of work.			

Scope of Work

A. Security Audit of the Oil Industry Development Board Bilingual (Eng. & Hindi) website:

1. Audit/Security update of OIDB website (www.oidb.gov.in) based on the Guidelines for Indian Government Websites.
2. Checking if commonly known holes in the website exist.
3. The audit has to be done on the following parameters -
   - ➢ To Assess Flaws in the Design of the website.
   - ➢ Attempting to guess passwords using password-cracking tools.
   - ➢ Validations of various data inputs.
   - ➢ Exception handling and logging.
   - ➢ Logical access control and authorization.
   - ➢ Evaluate the environment under which the website /application runs.
   - ➢ An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.
   - ➢ Malicious modification of data.
   - ➢ Website/ Application Security Audit
   - ➢ Compliance Review

4. The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website "Certified for Security".
5. Auditor must test website for attacks. The various checks/attacks/Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/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
   - ✓ PHP remote scripts vulnerability
   - ✓ HTTP Injection
   - ✓ Phishing a website
   - ✓ Buffer Overflows, Invalid inputs, insecure storage etc.
   - ✓ Any other attack that can be a vulnerability to the website or web applications.

6. The Top 10 Web applicationsecurity vulnerabilities, which are given below, Auditor should also check them, but not restricted to the following: -

6.1- Top Ten Most Critical Web Application Security Vulnerabilities in 2022		
A1	Broken Access Control	Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights
A2	Cryptographic Failures	Applications and APIs that don't properly protect sensitive data such as financial data, usernames and passwords, or health information, could enable attackers to access such information to commit fraud or steal identities.
A3	Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile datacan trick the interpreter into executing unintended commands or accessing unauthorized data
A4	Insecure Design	Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design". An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.
A5	Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application
A6	Vulnerable and Outdated Components	Developers frequently don't know which open source and third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. Attackers can exploit an insecure component to take over the server or steal sensitive data.

A7	Identification and Authentication Failures	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities
A8	Software and Data Integrity Failures	Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations
A9	Security Logging and Monitoring Failures	The time to detect a breach is frequently measured in weeks or months. Insufficient logging and ineffective integration with security incident response systems allow attackers to pivot to other systems and maintain persistent threats
A10	Server-Side Request Forgery	SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

Other Details of OIDB Website:-

S.No.	Parameters	Description
1.	Web Application Name & URL	http://www.oidb.gov.in/
2.	Will the website be hosted on NIC Server/ SDC or other - Please specify?	NIC Server
3.	Is the website on Intranet or Internet?	Internet
4.	Application Development Environment	Microsoft Visual Studio ,.Net Framework 4.0
5.	Processors	Intel®Xeon ® CPU E5-2640v2@2.00Ghz
6.	Operating System Details (E.g. Windows-2003, Linux, AIX, Solaris, etc.)	Windows Server 2012
7.	Front-end Tool [Server-side Scripts] (E.g. ASP, Asp.NET, JSP, PHP, etc.)	Asp.net C#
8.	Back-end Database (E.g. MS-SQL Server, PostgreSQL, Oracle, etc.)	MS-SQL Server 2012

B. Security Audit Report:

The website 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 the standard for Audit, if any.
4. Audit plan.
5. Additional mandatory or voluntary standards or regulations applicable to the Auditee.
6. Audit Standards should be followed.
7. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
   i) Tools used
   ii) List of vulnerabilities identified
   iii) Description of vulnerability

iv) Risk rating or severity of vulnerability
v) Test cases used for assessing the vulnerabilities
vi) Illustration if the test cases to provide the vulnerability
vii) Applicable screen dumps

8. Analysis of vulnerabilities and issues of concern.
9. Recommendations for action.
10. Personnel involved in the audit.

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

C. Objectives:

1. To conduct security audit to assess vulnerabilities to the OIDB Website i.e. www.oidb.gov.in as per the Guidelines of Indian Government website and rectification of vulnerabilities. The audit shall be conducted to review/identify the intent and vulnerabilities to the OIDB's website.

2. To identify the corrective measures and rectification of the vulnerabilities in www.oidb.gov.in website.

D. Deliverables:

1. The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.

2. Compliance review should be done by the agency after ensuring that changes to remove the vulnerabilities are completed.

3. Compliance audit should be done not only to check for removal of previously identified threats but also to ensure that the application or website has no vulnerabilities as result of changes done in the code and the vulnerability score should be above 80%.

Annexure- II

Terms & Conditions

1. **Time Schedule:**

S. No.	Deliverables	Duration (Fromthe date of issue of work order)
1.	The first round of audit report should be submitted to OIDB.	**10-15 working days**
2.	The consecutive round reports if any, should be submitted to OIDB.	**1 week working days**

2. **Indemnity Clause:**
   The Vendor will protect and save OIDB against all claims, Audit Error, Security Issue, and other proceedings resulting from infringement of any provision related to or in respect of Audit Certificate.

3. **Bid Validity Period**: a) Validity of bid should be 45 days from the date of opening of Technical Bid. Bids with validity less than 45 days shall not be considered.

   b) Bids received without the prescribed Earnest Money Deposit for an amount equal to 3% of the contract value shall be rejected.

   c) EMD waiver for SMEs/MSMEs will be as per government guidelines. A certificate of SME/MSME status will be required mandatorily.

   d) EMD of the unsuccessful tenderer will be returned, without interest, within a period of two (2) months from the date of award of contract to the successful bidder.

   e) EMD of the successful bidder will be adjusted against the security deposit/performance security deposit as per bidder's consent.

   f) EMD of the successful bidder shall liable to be forfeited if the bidder does not sign an agreement in the prescribed form attached within ten (10) days of the receipt of the letter of Award (LOA).

4. **Corrupt or fraudulent practices:**
   a) The Service provider shall observe the highest standard of ethics during the execution of the contract.
   b) The service provider shall ensure that there is no misuse or fraudulent practices with data.
5. **Terms of payment:**
   a) 100% payment will be made only after submitting the final security audit certificate issued by Cert-In on completion of Audit of OIDB's bilingual (www.oidb.gov.in) website.

   b) Under no circumstances any extra/ additional taxes, duties, levies etc. shall be payable to the bidder by OIDB unless such a tax, duty or levy has been newly introduced and notified by the Government of India.

c) Payment will be released through NEFT/RTGS in favour of bidder, after successful Audit of OIDB website.

6. Penalty clause:

a) For the delayed completion OIDB shall be entitled to recover the amount equal to 1% of the total work order value per day subject to maximum 10% of contract value OIDB shall also be at liberty to cancel the work order & get the job done at your risk and cost.

7. Submission of EPBG (Electronic- Performance Bank Guarantee) :

E- Performance Bank Guarantee within seven days (7) from the date of issue of work order as per attached Format or Demand Draft or Fixed Deposit Receipt (in original) made in favour of OIDB for an amount equal to 5% of the contract value. Performance security/SD shall remain valid for a period of 60 days beyond the date of completion of all contractual obligations.

8. Arbitration:

Dispute, if any, arising out of the contract, shall be settled by mutual discussion, failing which, the dispute shall be referred to arbitrator to be appointed by Secretary, OIDB and arbitration shall be considered as per Arbitration Act. Notwithstanding the place where the work under this contract is to be executed, the courts of Delhi alone shall have the jurisdiction over all matter concerning this contract.