

REQUEST FOR PROPOSAL (RFP)
FOR
Information Security Audit of MPCB Website.

Maharashtra Pollution Control Board.

3rd & 4th Floor, Kalpataru Point,
Near Sion Circle, Sion, Mumbai 400022
Maharashtra.

<http://www.mpcb.gov.in>

Contents

1	Section 1: Instructions to Bidders	4
1.1	Introduction and Background	4
1.2	Objectives	4
1.3	Submission of Proposals	5
1.3.1	The proposals shall be submitted in a two-cover format:	5
1.3.2	General conditions for tender bid submission:	5
1.3.3	Special condition for the tender:	6
1.3.4	Eligibility Criteria for Bidders	6
1.3.5	Technical Proposal	7
1.3.6	Financial Proposal	7
1.3.7	Disqualifications	8
1.4	Evaluation Process	8
1.4.1	Technical Evaluation:	8
1.4.2	Financial Bid Evaluation	9
1.5	Award and Duration of the work	9
1.5.1	Subcontracting and/or Outsourcing of Work	9
1.6	Termination of the Work	9
1.7	Penalties	9
1.8	Payment Terms and Conditions	10
1.8.1	Payment Schedule:	10
1.9	Performance Guarantee	10
1.10	Audit Environment	10
1.10.1	Responsibilities of the auditor	10
1.10.2	Quality Of Audit	11
1.10.3	Confidentiality and copyright	11
1.11	Validity of Proposals	11
1.12	Right to Accept/Reject Proposals	11
1.13	Clarifications and amendments of RFP Document	11
1.13.1	RFP Clarifications	11
1.13.2	Amendments in RFP	11
1.14	Arbitration	12

Information Security Audit - Request for Proposal

2	Section 2: Terms of Reference	12
2.1	Scope of the Work	12
2.1.1	Task 1: Web Application Test.....	12
2.1.2	Task 2: Patching of the application.	13
2.1.3	Task 3: Re, Re-Audit, Re- Re-patching	13
2.1.4	Task 4: Reporting.	13
2.2	Deliverables and Audit Reports.....	15
2.2.1	General:	15
2.2.2	Application Audit:	15
2.2.3	Application Patching:	15
2.2.4	Timeframe of the deliverables.....	16
2.3	Application detail:	16
3	Annexure-1: Proposal covering letter.....	17
4	Annexure-2: Technical qualification Details.	18
4.1	General Information.....	18
4.2	Information about the Company	18
4.3	Financial Details as per Audited Balance Sheet	18
5	Annexure 3: Proposal Format Sheet:.....	20
6	Annexure 5: PROFORMA OF PBG	21

1 Section 1: Instructions to Bidders

1.1 Introduction and Background

Maharashtra Pollution Control Board (MPCB) was established on 7th September, 1970 under the provisions of Maharashtra Prevention of Water Pollution Act, 1969. The entire state of Maharashtra has been declared as Air Pollution Control Area since 6.11.96. MPCB is also functioning as the State Board under section 5 of the Air (P&CP) Act, 1981. Maharashtra Pollution Control Board (MPCB) is implementing various environmental legislations in the state of Maharashtra, mainly including Water (Prevention and Control of Pollution) Act, 1974, Air (Prevention and Control of Pollution) Act, 1981, Water (Cess) Act, 1977 and some of the provisions under Environmental (Protection) Act, 1986 and the rules framed there under like, Biomedical Waste (M&H) Rules, 1998, Hazardous Waste (M&H) Rules, 2000, Municipal Solid Waste Rules, 2000 etc. MPCB is functioning under the administrative control of Environment Department of Government of Maharashtra.

Environment Information Centre (EIC) has over the years developed the MPCB website which is updated and maintained on a daily basis. The MPCB website makes it possible for the consent applications to be submitted at the respective Regional/ sub Regional Offices. To maintain transparency the website has a very important role to play by providing easy web-based access to the updated information related to Consent Granted, consent pending and consent refusal, on a daily basis.

A secure web portal mitigates risk of unauthorized access to resources, has an auditable trail to support transactions, particularly those with high sensitivity, protects important information from the moment it is entered by the user and as it continues through backend applications and workflow processes, strengthens on-line relationships enabling more and more applications and services to be integrated with and accessed via the high-value web portal applications. Also submission of data on a web portal to its final destination in multiple back-end applications, information needs to be protected from unauthorized access or use.

EIC wants to ensure that the MPCB web application has the C-I-A parameters well established and in this context is requesting this proposal from auditing and development firms to audit and thereof patch the web application.

1.2 Objectives

The first objective of this request for proposal (RFP) is to conduct the Audit to discover all vulnerabilities/weaknesses/attacks in the web Based Applications. The Audit should be done by using Industry Standards and at minimum check for the top 10 vulnerabilities listed by Open Web Application Security Project (OWASP).

The second objective of this RFP is to patch and harden the application so as to satisfy the auditor that no vulnerability remains in the application, as of the date of the audit. Most importantly the functionality and availability of the application is not impacted during the patching.

The final objective is getting the application certified by the auditor stating “fit for hosting” and the said certificated has be acceptable to NIC/Cert-in.

1.3 Submission of Proposals

1.3.1 The proposals shall be submitted in a two-cover format:

1.3.1.1 Contents of cover 1

1.3.1.1.1 Technical Bid

1.3.1.1.1.1 Technical Qualification details, EMD and supporting documents.

1.3.1.1.1.2 The EMD will be of value INR 10,000.00

1.3.1.1.2 Contents of cover 2

1.3.1.1.3 Financial bid.

1.3.1.1.3.1 Financial proposal as per Annexure-3.

The Bidder shall submit Bid along with a demand draft of Rs. 10,000/- in the name of MPCB Mumbai as an EMD and the Technical Bid in one envelope and Financial Bid documents in separate wax sealed envelope prescribing Technical and Financial Bid on the top left hand corner respectively. The two sealed covers envelopes are to be put in a bigger cover which should also be sealed and dully super scribed:

MPCB Web Application Tender.

Tender Number

Due Date:

Bid Opening Date:

The EMD shall carry no interest and will be returned to all the unsuccessful bidders on the contract being awarded or scrapped. The EMD will be returned to the successful bidder on issuance of PBG. The date and time of collection of EMD will be notified to the Bidders, stating the time in which it may be collected.

1.3.2 General conditions for tender bid submission:

1.3.2.1 All proposals should be submitted in English language only

1.3.2.2 MPCB reserves the right to reject any or all offers and discontinue this tender process without obligation or liability to any potential Bidder

1.3.2.3 All proposals received after the specified date and time shall not be considered for award of work.

1.3.2.4 The Proposals received by fax or email shall be treated as defective, invalid and rejected.

1.3.2.5 The original and copies of the bid, each consists of the documents listed in instructions, shall be typed and shall be signed by the bidder or a person(s) duly authorized to bind the bidder to the contract.

1.3.2.6 MPCB reserves the right to place an order separately for auditing and patching, as deemed beneficial to MPCB.

1.3.3 Special condition for the tender:

- 1.3.3.1 The principle bidder for this tender can either be a Cert-in Empanelled company or software development company with CMMI level 3(or above) maturity level.
- 1.3.3.2 The audit of the application and there-after fit for hosting certificate will be issued by the Cert-in empanelled company.
- 1.3.3.3 The patching of the application will not be done by the auditing (the company which is auditing the application) company thereby maintaining segregation.
- 1.3.3.4 The patching of the application must be done by a different Cert-in empanelled company or CMMI level 3 (or above) company.
- 1.3.3.5 The auditor certifying the audit work must be a CISSP.
- 1.3.3.6 The team/Project leader of the firm patching the application must be a CISA.
- 1.3.3.7 In general the company auditing the application will not patch the application and vice versa.
- 1.3.3.8 If the principle bidder is the auditing company, then it shall get the application patched by a CMMI Level 3 (or above) development firm. The CISA auditor of the development firm will certify that the application has been patched as per the SOX guidelines (relating to segregation of duties).
- 1.3.3.9 If the Principle bidder is the development firm, it shall get the application audited and certified from a Cert-in Empanelled organization and the auditor must be a CISSP.
- 1.3.3.10 **Note:** In this RFP document, the following wordings will be used for easy reference:
 - 1.3.3.10.1 **Auditing Vendor:** *The firm which is going to audit the application.*
 - 1.3.3.10.2 **Patching Vendor:** *The firm which is going to patch the application*

1.3.4 Eligibility Criteria for Bidders

The audit firms that qualify the below mentioned criteria need only apply.

- 1.3.4.1 This invitation is open to all Indian firms/company (the bidder).
- 1.3.4.2 The firm/company must be a company registered under the Indian Companies Act, 1956/ The Partnership Act, 1932 or Registration of Societies Act.
- 1.3.4.3 The bidder must have been empanelled by CERT-IN or a CMMI level 3 company having the requisite certificate valid up to 31st Aug 2015. Proof of this will have to be submitted.
- 1.3.4.4 The bidder should have been in operation for a period of at least 3 years as of 31-3-2014 as evident by the Certificate of Incorporation and Certificate of Commencement of Business issued by the Registrar of Companies, India.
- 1.3.4.5 The bidder should have had an average annual turnover of at least (Rs) **25,00,000/-** (Twenty five Lakhs) during the last 3 financial years in Information Technology (IT)

Information Security Audit - Request for Proposal

related operations i.e. for the financial years 20010-11, 2011-12 & 2012-13 as revealed by audited accounts.

- 1.3.4.6 The bidder should have Certified Information Systems Auditor (CISA / CISSP qualified professionals so as to associate with the audit team or the patching team, as required.
- 1.3.4.7 The bidder should have experience of conducting similar Web Applications audit for a government agency wherein the segregation of duty was maintained, with respect to auditing and patching.
- 1.3.4.8 Where the firm patching the application is not Cert-in empanelled and is the principle bidder, then it must have experience of at least one government project, in the FY year 2013-14, of value not less than INR 5 Lac, whereby the application Audit project stands completed. The firm should have obtained a “fit for hosting” certificate from a Cert-in Empanelled company/firm.
- 1.3.4.9 The bidder should have to submit the proof for the eligibility criteria including Sales Tax Registration, Income Tax PAN Number and Etc.,

1.3.5 Technical Proposal

The Technical Bid shall include the detailed project plan for Audit of the web Applications , The project plan should indicate the milestones and time frame of completion of the different activities of the project. The bidder is required to give details of the Project Management Methodology, Audit Standards and methodology. Resources and support required from MPCB may also be clearly defined. The technical bid is required to be submitted in the format as given in **Annexure 2**.

1.3.6 Financial Proposal

Following are the terms and conditions for the Financial Proposal:-

- 1.3.6.1 This tender is for a fixed price bid.
- 1.3.6.2 The financial proposal shall be priced in Indian Rupees.
- 1.3.6.3 The Financial proposal shall clearly indicate, as per the Financial Summary Sheet in **Annexure-3**, the total costs of carrying out the services as described in the Terms of Reference (TOR) as well as taxes namely Value Added Tax (VAT) and Service Tax etc wherever applicable.
- 1.3.6.4 The quotations shall be fixed and shall not allow for any fluctuation in costs. MPCB understands that the vulnerability quantum is variable, irrespective, MPCB expects the bidder to be knowledgeable in effort estimation of such projects. MPCB does not wish to deploy inexperienced auditors who are not capable of estimating the patching work.

1.3.7 Disqualifications

MPCB may at its sole discretion and at any time during the evaluation of Proposal, disqualify any bidder, if the bidder has:

- 1.3.7.1 Submitted the Proposal documents after the scheduled date and time;
- 1.3.7.2 Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;
- 1.3.7.3 Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years;
- 1.3.7.4 Submitted a proposal that is not accompanied by required documentation or is non responsive;
- 1.3.7.5 Failed to provide clarifications related thereto, when sought;
- 1.3.7.6 Submitted more than one Proposal;
- 1.3.7.7 Declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices or blacklisted.
- 1.3.7.8 Submitted a proposal with price adjustment/variation provision.
- 1.3.7.9 EMD of disqualified bidders will not be returned and the said amount will stand confiscated.

Please note that the MPCB reserves the right to carry out the capability assessment of the “Bidder” and that the decision of MPCB shall be final in this regard.

1.4 Evaluation Process

A two stage procedure (i.e. Technical Bid and Financial Bid) will be opted for evaluation of proposals. The process for evaluation of proposals is as given below:

1.4.1 Technical Evaluation:

Technical Proposals would be opened only for those bidders who have submitted as per the tendering schedule. An Evaluation Committee will assess all the bids received. Preliminary scrutiny of the Proposals for eligibility will be done to determine whether the Proposals are complete, whether the documents have been properly signed, whether any computational errors have been made, and whether the Proposals are generally in order. Proposals not conforming to qualification eligibility criteria shall be rejected summarily. Non-conforming Proposals shall be outrightly rejected.

The bid will be rejected if there is no EMD along with the technical bid.

If a Technical Proposal is determined as not substantially responsive, MPCB will reject it. Technical Proposals conforming to technical bid format will be taken up for detailed Technical evaluation. All the bidders who have submitted correct Technical bid documents in compliance with all the requirements will be declared as technically qualified for this bid with MPCB.

1.4.2 Financial Bid Evaluation

Only technically qualifying bidder would be eligible for financial bid evaluation. The evaluation of the financial proposals shall be carried out considering the total cost of the project to MPCB, as indicated in the formats suggested for furnishing the Financial Bids vide **Annexure -3**.

MPCB may, at their discretion and without explanation to the prospective Bidders, at any time choose to discontinue this tender without obligation.

1.5 Award and Duration of the work

On acceptance of Proposal for awarding the contract, MPCB will notify the successful bidder in writing that their proposals have been accepted. MPCB and successful bidder shall sign the Contract Agreement. No variation in or modification of the term of the Contract shall be made thereafter except by written amendment signed by the parties.

The successful bidder will be given a period of 15 days to start the work. The successful bidder is expected to complete the work within a period of **145 calendar days** after the start of work. This time period includes the time taken by the development firm to rectify the identified vulnerabilities. EIC may use is discretionary judgment to alter the delivery date, however such a decision/activity is not binding on MPCB.

1.5.1 Subcontracting and/or Outsourcing of Work

The principle bidder (Vendor) will not Outsource / subcontract their scope of work, i.e. either auditing or patching the application. The vendor will inform MPCB of the party to whom the auditing or patching work respectively has been outsourced, before sharing the application code/access/vulnerability report. For example if the principle bidder (vendor) has opted for performing the audit function, then this principle bidder cannot outsource the auditing task, as such, the CISSP auditor must be an permanent employee of the principle bidder. The principle bidder in this case will inform MPCB of the application development company which will do the application patching work, before giving the development company access to the vulnerability report and application code. The CISA auditor and the application development team must be permanent employees of the CMMI level 3 (or above), application development firm.

1.6 Termination of the Work

MPCB without prejudice to its rights under the Conditions of tender or any other remedy for break of Contract, shall have the right to terminate contract at any time, if, the bidder or its appointed associate breaches any of the terms and conditions:

- 1.6.1. Mentioned in this document or in the Award of Contract;
- 1.6.2. As defined by CERT-IN, Department of Information technology, Min .of Information Technology, Government of India
- 1.6.3. The contract may also be terminated in case, MPCB is of the view that the Auditor's performance or competence fails to meet the standards required for the Audit assignment.

1.7 Penalties

For any delay in completion of the task beyond five months period from the date of award of work, the liquidated damages of a sum equivalent to 0.5% of the project value for every day of delay, up to

Information Security Audit - Request for Proposal

a maximum of 15% of the contract value shall be deducted from the project value. Once the maximum, penalty amount is reached, the contract will be terminated.

1.8 Payment Terms and Conditions

- a. The bidder will offer commercial quote, based on fixed cost, inclusive of VAT, Service Tax etc. and other duties, cess, fees etc., if any and MPCB will not pay any additional amount other than indicated in the offer.
- b. TDS will be deducted at source for any payment made, as per rules of Government of India.
- c. MPCB will neither provide nor reimburse expenditure towards any type of accommodation, travel ticket, airfares, train fares, halting expenses, transport, lodging, boarding etc.
- d. The audit firm/company shall keep information related to this project confidential and will not divulge to outside agencies without written consent from MPCB.

1.8.1 Payment Schedule:

- 1.8.1.1 60% of the contract value on submission of Level 1 audit report.
- 1.8.1.2 40% of the contract value on MPCB acceptance of “fit for hosting certificate” or Application hosted by NIC and submission of all the reports.

1.9 Performance Guarantee

The successful bidder shall furnish the performance security representing 15% of the total value of the contract within 15 days of the receipt of notification of award as per the Performance Bank Guarantee Form provided in Annexure-5

Performance security should remain valid for a period of three months beyond the date of completion of all contracts.

1.10 Audit Environment

The Web-application Audit may be conducted at the successful bidder's site by accessing it remotely. MPCB can also share the application code with the vendor. It is the responsibility of the vendor to collect the source code securely from EIC. The successful bidder shall agree with the Non-Disclosure Agreement (NDA) as specified in this RFP.

1.10.1 Responsibilities of the auditor

While submitting the audit report and patched application to MPCB the Auditor shall ensure that:

Information Security Audit - Request for Proposal

- 1.10.1.1 The auditing is carried out strictly in accordance with the terms and conditions stipulated in the audit assignment contract as well as general expectations of the auditee from an auditor.
- 1.10.1.2 All applicable codes of conduct and auditing standards are adhered to with due professional care.
- 1.10.1.3 Patching of the application does not affect the availability aspect of the application.

1.10.2 Quality of Audit.

The selected vendor will ensure that the audit assignments are carried out in accordance with applicable guidelines and standards as mentioned in this document and terms and conditions specified by the CERT-IN, Department of Information Technology, Min. of Information Technology, Government of India.

1.10.3 Confidentiality and copyright

Information relating to the examination, clarification and comparison of the Proposals shall not be disclosed to any bidder or any other persons. The undue use by any bidder of confidential information related to the process may result in rejection of its proposal. During the execution of the project, except with the prior written consent of the MPCB, the Consultant and its personnel shall not at any time communicate to any person or entity, any confidential information acquired in the course of the auditing. All recipients of tender documents, whether they submit a tender or not, shall treat the details of the documents as private and confidential. Copyright in the documents prepared by the bidder is reserved with MPCB. The Auditor shall ensure that his employees, servants keep confidential all information in whatever form it is obtained, produced or derived from or related to the carrying out of its obligations under this terms and conditions as well as the Contract with MPCB.

1.11 Validity of Proposals

The bidder proposal shall remain valid for a period of **120** days beyond the closing date of the tender.

1.12 Right to Accept/Reject Proposals

MPCB reserves the right to accept or reject any Proposal(s) at any time prior to award of contract, without thereby incurring any liability to the affected Respondent(s) or any obligation to inform the affected bidder (s) of the grounds for such decision.

1.13 Clarifications and amendments of RFP Document

1.13.1 RFP Clarifications

During Technical Evaluation of the Proposals MPCB may, at its discretion, ask bidders for clarifications on their proposal. The bidders are required to respond within the prescribed time frame as specified by MPCB, failing which their respective bids may be rejected.

1.13.2 Amendments in RFP

At any time prior to deadline for submission of proposal, MPCB if may for any reason, modify the

Information Security Audit - Request for Proposal

RFP, the prospective bidders having received the RFP shall be notified of the amendments through website and/or newspapers and such amendments shall be binding on them.

1.14 Arbitration

In the event of a dispute or difference of any nature whatsoever between the Audit firm/company and MPCB during the course of the assignment arising as a result of this order, the matter shall be referred to Arbitration as per Arbitration & Reconciliation Act, 1996

2 Section 2: Terms of Reference

2.1 Scope of the Work

Bidders would be expected to perform the following tasks:

1. Application Security Testing, re-testing to confirm closure of Vulnerability.
2. Patching of application based on vulnerability report.
3. Issuance of "Fit for Hosting" certificate as per NIC guidelines.

The deliverable is a secure application fit for hosting at NIC, as per NIC guidelines without affecting the functionality of the original application.

2.1.1 Task 1: Web Application Test

The Top 10 Web application vulnerabilities (as per OWASP), which are given below, should be checked up for the given web applications at minimum:

1. Cross Site Scripting(XSS)	XSS occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, insert hostile content, conduct phishing attacks and take over the user's browser using scripting malware.
2. Injection Flaws	<i>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.</i>
3. Insecure Remote File Inclusion	Code vulnerable to remote file inclusion allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise.
4. Insecure Direct Object reference	A direct object reference occurs when a developer expose a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attacker can manipulate those references to access other objects without authorization.
5. Cross site request Forgery (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 benefit of the

Information Security Audit - Request for Proposal

	attacker.
6. Information leakage and Improper Error handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use the weakness to violate privacy, or conduct further attacks.
7. Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume user's identity.
8. Insecure Cryptographic Storage	Web applications 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.
9. Insecure communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
10. Failure to Restrict URL Access	Frequently, the only protection for sensitive areas of an application is links or URLs are not presented to authorized users. Attackers can use this weakness to access and perform unauthorized operations.

The applications have to be tested for Functional application security as well.

2.1.2 Task 2: Patching of the application.

- 2.1.2.1 The consortium partner of the principle bidder will be responsible to patch the application for all the vulnerabilities listed in task 1.
- 2.1.2.2 Before starting the application patching a minimum of 100 sample functionality check points will be established. The input and output result of these checkpoints will be recorded/documented. The principle bidder will submit this functional test report to MPCB.
- 2.1.2.3 The time taken by MPCB to approve the sample functionality check points for adequacy and sample spread will not be adjusted towards project completion time lines. Making of this checklist should be done parallel to task 1.

2.1.3 Task 3: Re, Re-Audit, Re- Re-patching

If vulnerabilities are observed from the re-audit, the consortium partner will re-patch the application and this cycle will continue till all the vulnerabilities have been mitigated.

2.1.4 Task 4: Reporting.

When the application code is being modified, the principle bidder will send the updated/changed application code to EIC, preferably every Monday. Only the modules which have been updated will be sent. It is the responsibility of both the parties working on the application to check the application for preserving its functionality. Sending the code to MPCB does not imply that MPCB will be responsible to verify the application code functionality or acceptance of application patching.

2.1.4.1 Task 5: Testing.

On completion of audit and application patching the vendor will check the impact of patching for availability and integrity. The sample functionality check points made during the task2 stage will be used to verify any

Information Security Audit - Request for Proposal

functionality issue. This test report will be submitted to MPCB.

2.2 Deliverables and Audit Reports

2.2.1 General:

- (a) The responsibility of submitting all reports is attributed to the Principle bidder. The signature on the reports/certificate(s) submitted by the auditor, CISSP, will be on his/her company letterhead.
- (b) The signature on the reports submitted by the developer, CISA, will be on his/her company letterhead.

2.2.2 Application Audit:

- 2.2.2.1 The vendor will be required to submit the following documents after the application audit:
- 2.2.2.2 A detailed and summary report will be submitted detailing the discovered vulnerabilities, the impact of the vulnerability with associated risk levels and recommendations for risk mitigations. The detailed report will also give the steps/method used to establish the vulnerability along with screen-shots.
- 2.2.2.3 For a given vulnerability all possible links affected in the application will be specified.
- 2.2.2.4 All deliverables shall be in English language and side A4 size format.
- 2.2.2.5 For re-audit reports the previous level summary report needs to be updated, giving the audit level and the updated status of the vulnerability (open/closed). In the event a new vulnerability is determined at a re-audit level a new summary table for that level will be made and in the detailed report the auditor will specify the reason for finding vulnerability at a re-audit stage.
- 2.2.2.6 The auditing vendor will submit the audit report at every stage to MPCB. The report will be mailed to EIC. This is a measurable parameter for the project progress.
- 2.2.2.7 The clearance certificate for, "Fit for Hosting" as per NIC guidelines and certified (stamped and signed) CD/DVD of the security cleared application.

2.2.3 Application Patching:

- 2.2.3.1 Sample functional test points, a minimum of 100 test points, will be submitted to MPCB for approval.
- 2.2.3.2 Patch Application report for covering each rectification done in the application will be submitted to MPCB and the auditing vendor, for each audit level. This report is a measurable criterion for project progress and also for QA.
- 2.2.3.3 After the auditing vendor has informed over the mail that all vulnerabilities have been closed in the application, the patching vendor will submit the functional test report to MPCB and the auditing vendor.
- 2.2.3.4 The secure application on a CD/DVD, the hash codes of all the files and the hash algorithm will be submitted to the Auditing vendor.

2.2.4 Timeframe of the deliverables

- 2.2.4.1 The selected successful bidder will be required to start the project within 15 days from the date of placing the order for the audit.
- 2.2.4.2 The entire audit must be completed within 145 calendar days from the date of placing of order.
- 2.2.4.3 All the reports of the agreed deliverables should be submitted by the firm/company within **15** days of the completion of the audit.
- 2.2.4.4 The audit, as mentioned above, has to be completed in time. It is expected that, if required, the successful bidder may deploy multiple teams to complete the audit projects within given time frame.

2.3 Application detail:

- 2.3.1. Web Application : <http://www.mpcb.gov.in/index.php>
- 2.3.2. Application type: Dynamic.
- 2.3.3. Type of Access: Generic User Access to/ folder.
- 2.3.4. Good approximation of number of Dynamic pages: 260
- 2.3.5. Good approximation of number of Static pages: 90
- 2.3.6. Number of Parameters: 4600.

The above estimate includes the web pages and its CMS.

3 Annexure-1: Proposal covering letter

Letter Dated Date/Month/Year

**I/C Environment Information Centre.
Maharashtra Pollution Control Board.**

3rd & 4th Floor Kalpataru Point
Near Sion Circle, Sion, Mumbai 400022
Maharashtra.

Dear Sir,

Re: Web application Security audit and patching for MPCB.

In response to the RFP for “Web audit and patching of MPCB web site”, we herewith submit our proposal. The following documents have been included as part of the proposal:

S.NoEnclosed documents

- 1 Technical bid and EMD (sealed and marked)
- 2 Commercial bid (sealed and marked)
- 3 Additional Information if any

Sincerely yours

(signature) (In the capacity of)

Duly authorized to sign the tender response for and on behalf of:

(Name and Address of Company) seal/stamp of bidder

4 Annexure-2: Technical qualification Details.

4.1 General Information

Name of the Company:
Details to be furnished of only the Prime Bidder
Address Telephone/Mobile Fax Email Website
Details of Authorized person
Address
Telephone
Mobile
Email.

Prime Bidder responsibility in the tender: Application Audit/ Application Patching (Select One).

4.2 Information about the Company

- 4.2.1. Is the firm/company registered under the Indian Companies Act, 1956, The Partnership Act, 1932 and the Registration of Societies Act?
 - 4.2.1.1. Give Page no. Where proof is given
- 4.2.2. Has the firm/company been in operation for a. period of at least 3 years as of 31.4.2014?
 - 4.2.2.1. Give Page no. Where proof is given
- 4.2.3. Has the firm/company provided self attested copies of the following valid documents?:
 - 4.2.3.1. Provident Fund No
 - 4.2.3.2. PAN No.
 - 4.2.3.3. Service Tax Registration No.
 - 4.2.3.4. Income Tax Registration No.
- 4.2.4. Applicable for firms auditing the application and is the principle bidder.
 - 4.2.4.1. Does the Firm/Company have Empanelment as an IT Security Auditor by CERT-IN (Valid Upto 31st Aug 2015?)
 - 4.2.4.2. Details of CISSP Auditor
- 4.2.5. Applicable for firms patching the application and is the principle bidder.
 - 4.2.5.1. Does the Firm/Company have SEI CMMi Level 3 Certification?
 - 4.2.5.2. If this principle bidder firm not Cert-in empanelled then it details of work experience as specified in eligibility criterion needs to be submitted
 - 4.2.5.3. Details of CISA auditor

4.3 Financial Details as per Audited Balance Sheet

- 4.3.1. Does the firm/company have an average turnover of (Twenty-five Lakhs) during the last 3 financial years in Information Technology related Projects as revealed by audited accounts?
 - 4.3.1.1. Year Turnover
 - 4.3.1.1.1. 20010-11
 - 4.3.1.1.2. 2011-12

Information Security Audit - Request for Proposal

4.3.1.1.3. 2012-13.

(Proof of this need to be Give. Page no. Where proof is given)

4.3.2. **Total Turnover** (the last three years in Information Technology related operations):

Give Page no. where proof is given

4.3.3. Describe Project implementation Methodology giving approach of vendor along with rollout plan, Project Management and Reporting.

4.3.4. Describe Level of skills and experience

5 Annexure 3: Proposal Format Sheet:

Sr.No		Carrying out Security Audit		Cost in Rupees
1	Applications audit			Rs.
2	Application Patching			Rs.
5		*Cost on account of Taxes:		
		Service Tax		Rs.
		Any other Taxes		Rs.
				Rs.
6		**Grand Total Cost:		Rs.
			*Please show the calculation of taxes along with applicable rate of taxes.	

6 Annexure 5: PROFORMA OF PBG

GUARANTEE BOND

Ref : _____ Date _____

Bank Guarantee No. _____ To _____

MPCB

1. Against contract vide Advance Acceptance of the Tender

No. _____ dated _____ of I/c Environment Information Centre (hereinafter called "the Department") covering "IS AUDIT" to be implemented in Mumbai (hereinafter called the "said contract") entered into between the Department and _____ (hereinafter called the "Tenderer"), this is to certify that at the request of the Tenderer we _____ Bank are holding in trust in favor of the Department, the amount _____ (write the sum here in words) to indemnify and keep indemnified the Department against any loss or damage that may be caused to or suffered by the Department by reason of the said contract and/or in the performance thereof. We agree that the decision of the Department, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the Tenderer and the amount of loss or damage that has been caused or suffered by the Department shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Department.

2. We _____ Bank further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfillment in all respects of the said contract by the

Tenderer i.e. till _____ (viz the date upto 3 months after the date of successful implementation and acceptance of the Audit Report by the Department) hereinafter called the said date and that if any claim accrues or arises against us _____ Bank by virtue of this guarantee before the said date, the same shall be enforceable against us _____ Bank notwithstanding the fact that the same is enforced within one months after the said date, provided that notice of any such claim has been given to us _____ Bank by the department before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Department.

3. It is fully understood that this guarantee is effective from the date of the said contract and that we _____ Bank undertake not to revoke this guarantee during its currency without the consent in writing of the Department.

4. We undertake to pay the Department any money so demanded notwithstanding any dispute or disputes raised by the Tenderer in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal.

The payment so made by us under this bond shall be a valid discharge of our liability for payment there under

Information Security Audit - Request for Proposal

and the Tenderer shall have no claim against us for making such payment.

5. We _____ Bank further agree that the Department shall have the fullest liberty, without affecting in any manner our obligation hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Tenderer from time to time or to postpone for any time or from time to time any of the powers exercisable by the Department against the said Tenderer and to forbear or enforce any of the terms and conditions relating to the said contract and we, _____ Bank shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Tenderer or for any forbearance by the Department to the said Tenderer or for any forbearance and/or omission on the part of the Department or any other matter or thing what-so-ever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

6. _____ This guarantee shall not be discharged due to the change in the constitution of the Bank or the Tenderer.

Date _____

Place _____ Signature _____

Witness _____ Printed Name: -----

s common seal)