Government of N.C.T of Delhi
Department of Information Technology
9th Level, 'B' – Wing , Delhi Secretariat ,
IP Estate, New Delhi – 110 002

E-mail : progit@nic.in, Website:it.delhigovt.nic.in ***Phone: 011-23392074 Fax: 011-23392402***

Clarifications on Queries for REQUEST FOR PROPOSAL (RFP) FOR WEBSITE SECURITY AUDIT OF DELHI GOVERNMENT DEPARTMENTS, AUTONOMUS & LOCAL BODIES

Serial No.	Clause	Query	Answer
1	1.3.2 (i) Pre Qualification Criteria, "The bidder should have SEI CMM Level 5, or higher certificates".	We may like to mention here that CMM level is applicable to Software Development and not to Security Auditing. Thus, this condition is irrelevant and should be dropped.	**SEI CMM Level 5 is or higher certificates are not Mandatory. Condition Number (i) of clause no. 1.3.2 of RFP stands deleted.**
2	1.3.2(h) The bidder should have experience of conducting similar Website Audit as proposed by Department of Information Technology, Government of N.C.T. of Delhi of a minimum of 3 audit projects in organizations like banks, financial institutions, Insurance Companies or Government departments.	Kindly consider revision of this clause to 2 audit projects.	**This will be as per RFP.**
3	1.3.2(j) The bidder should own at least one commercial Security Audit Tool. Name, Description of the tool needs to be defined. Proof of this will have to be submitted.	1) Please note that most organizations in the web security audit business utilize free tools available readily in the market. These tools are equally competent in delivering the expected results. Please consider relaxation of this clause. 2) If relaxation does not happen, kindly specify the level of tools (in terms of price etc). This needs to be specified to maintain parity amongst the bidders, since, smaller players may opt for cheaper products which will lower the final bid cost. In such a scenario, we would request DIT to specify the requirements explicitly to ensure maintenance of highest-level standards. 3) Most of the website security auditing is done through freeware tools which are effective.	**Commercial Security Audit Tool is not mandatory. Condition Number (j) of clause no. 1.3.2 of RFP stands deleted**

		Thus, owning commercial security audit tool is not necessary and hence, this condition should be dropped. Moreover, we would like to know what proof needs to be submitted when the bidder is owning a commercial security tool.	
4	3.6) Annexure 6, Point 5 Provide Vendor's Proposed Technical solution: Type of Security assessment tool will be used for identifying Security Vulnerabilities tools (Licensed /Free) and Technologies	Earlier in the RFP it is mentioned that the vendor needs to have at least one Commercial Tool. Kindly clarify if free tools can be used to achieve the deliverables as mentioned in RFP instead of commercial tool.	**In view of the answered no. 03 given above, it is up to the bidder for selection of the Security Audit Tool (Commercial/License/Free). However, bidder will solely responsible for copyright / legal issues related to the tool chosen.**
5	Page 31, 3.1. Annexure-1 Notice of Intend to Bid.	Whether this notice has to be given along with the proposal. If not, then when the notice of intend to bid has to be given.	**The notice is to be given along with the proposal.**
6	The bidder should have been in operation for a period of at least 3 years as of 31-3-2007 as evident by the Certificate of Incorporation and Certificate of Commencement of Business issued by the Registrar of Companies, India	Since we started our operation in 2006. we don't meet this requirement.	**This is as per RFP**
7	Bidding in consortium	2. Is bidding in consortium allowed? As at one place in the document RFP, its denied (Page 8 of 56) and in the bidder details, its asking for the Bidder's Name together with consortium entity (Page 36 of 56).	**No consortium is allowed. Further, the word "Consortium" at serial no. 1 of the table of Clause No. 3.3, Annexure – 3 stands deleted.**
8	In "Main Objectives for." para 7 (pg 7) -	It needs to be clarified that this objective, i.e., to rectify/fix vulnerabilities, is not the responsibility of the bidder.(the vulnerabilities has to fixed up by the developer)	**The bidder will identify the vulnerabilities and the concerned department will rectify the identified vulnerabilities by the bidder.**
9	Section 8 Payment Schedule (pg 16) -	The payment schedule has been worked out based on various phases of the audit process, assuming that all the websites are audited in batch mode and they progress together in batches from phase to phase. But practically, the auditing will be done on individual websites separately and not in batches. Thus the progress of audit on various websites may be happening	**This is as per RFP.**

		at different paces. How will the payment schedule be worked out under such circumstances?	
10	1.10 Payment terms and conditions, Sub clause 4 1.9, &.9 penalties.	We would like the following modification to the clause 1.10 as highlighted and subsequently the clause 1.9 , penalties to be deleted :-Department of Information Technology, Government of N.C.T. of Delhi may impose penalty, in case of delay of any deliverables at the rate of 0.5% per week delay, either for completion of audit exercises or submission of draft reports, subject to a maximum of 30 % of the total cost *for that deliverable,* for all delays attributable directly to the Audit Firm/Company. Once the maximum penalty amount is reached, termination of the contract shall also be made.	**This is as per RFP.**
11	Section 2.2: Deliverables and Audit reports,	a.) Since removal of vulnerabilities is not under control of the bidder and also the re-audit cannot be started/completed without the removal of ALL vulnerabilities, how can the bidder commit to this time frame? b) It should be clarified whether the time-lines are mentioned in terms of working days or calendar days c)It is stated that the entire duration of the project is 180 days. Can you please clarify that this time period of 15 days is for which draft reports. d)The same is subject to the department permitting the two retests to be conducted within this time span with the 2nd test (if required) no later than 150 days after commencement of engagement Kindly clarify, if this expectation is appropriate, since the auditor is supposed to finish the review in 180 days.	**a.) The Department of IT will supplement the efforts of vendors to remove the vulnerabilities by the department.** **b) The timelines are in calendar days.** **c)180 days includes 15 days time period for draft reports.** **d) This is as per RFP**

12	At least One office in NCR:	We do not have an office in New Delhi. However, Punjab national bank is one of our largest customers and we have serviced the bank by deputing professionals to Delhi. Will we be eligible to apply?	**This is as per RFP.**
13	Sec 1.5 Evaluation process Technical Evaluation , Table, Technical Evaluation criteria, point 1 (b) Quality Management Standards/Certifications Five points are awarded for quality management standards and certification.	While an organization like ours hasn't been certified, we follow some of the most stringent quality and risk management practices owing to the nature of the professional services provided by us. Apart from a description of our internal quality & risk management processes pertaining to a typical security assessment engagement, what additional information is expected out of us in order to be fairly evaluated on this criteria?	**This is as per RFP.**

14	Sec 1.12 Audit Environment a) However the successful bidder needs to take the required permission from the particular Department. For this the successful bidder shall agree with the Non-Disclosure Agreement (NDA) as specified in this RFP. b) The successful bidder will also conduct a conference with the respective Departments/Corporations/Local Bodies in the Delhi Secretariat before the commencement of the work to understand the website of concerned Department. c) One visit to user department and meeting with representative of department is required to be done by auditor for guiding departments to fix/remove the vulnerabilities identified during the first audit by the Auditor.	In the interest of conserving time on these activities, will the following be deemed appropriate? a. A standard template will be prepared seeking a department's permission to assess its web sites. Prior to the commencement of the engagement, as part of the planning stage, all the departments will be requested to duly complete this template-based document with information relevant to their department. The template will require each department to identify the URLs of the department web sites to be assessed, provide a brief description of the site functionality, provide required credentials for the test accounts (where applicable), specify the details of the contact person for each web site, specify a time slot within the next week for initial meetings / discussions, and specify the preferred date of assessment along with time window for assessment. The project plan will be formulated only after this activity is completed) Conferences will be conducted with all the department personnel in the first week of the engagement post the signing off of the project plan. c) Post audit discussions with all the departments will be held one week after the submission of the draft report post the first assessment. All such discussions will be scheduled and completed within the same week. The engagement team will be onsite at Delhi for these discussions for one week.	**Comments are not required from the Bidder.**

15	**Section 1.15, Liability in respect of Damage** The Auditor shall make good or compensate for, all direct damage occurring to website and web applications of the respective department and/or Department of Information Technology, Government of N.C.T of Delhi in connection with this Contract for carrying out audit. Provided that this Clause shall not apply if the Auditor is able to show that any such damage is caused or contributed to by the neglect or default of the respective Department. The security auditor's liability will be limited to the cost of service provided. Default or neglect by the Auditor will include both malicious and non-malicious errors and project mismanagement.	The audit team will strictly adhere to the agreed upon assessment window and will restrict the assessment to pre-agreed vulnerability classes. Further, the auditee will also be advised to take up necessary precautions such as backing up of databases, application files, and system configuration prior to the assessment. However, owing to the inherent nature of the assessment, the potential for service disruption / system crash cannot be ruled out even though the auditor and the auditee have exercise due care. Hence, we cannot compensate for any damages that may arise out of our assessment as long as the assessment adheres to the agreed terms.	**Auditing will not be done on live websites.**
16	Section 1.24, Follow up and Compliance The Audit firm/company has to submit a summary compliance report at end of each task and the final report should be certify that the website/web applications (should be mentioned the name of the website and/or web applications) is **"**	Certified for Security ". Certify for security - We do not certify the applications for security. Instead, our report will state that the site was reviewed as per OWASP guidelines and the current status of the vulnerabilities identified are as documented in the report. If all the vulnerabilities are subsequently addressed, the report will indicate the current status of those vulnerabilities as 'Closed'. Note: We will perform two rounds of iteration as per the RFP.	**This is as per RFP.**
17	Section 2.1, Scope of work The auditor is expected to submit the final audit report after the remedies/recommendations are implemented.	The scope of work only entails a maximum of two iterations of tests post the initial assessment. Hence, the final report will be submitted after a maximum of two rounds of iterations post the initial assessment irrespective of whether the remedies / recommendations are appropriately implemented. We believe that the auditor is required to identify the vulnerabilities. The auditor can give suggestions to rectify the same. Based on the finding & suggestions given by auditor, DIT will have to contact the respective vendor to fix the	**This is as per RFP.** **The bidder will identify the vulnerabilities and the concerned department will rectify the identified vulnerabilities by the bidder.**

		Vulnerabilities.	
18	Section 3.14, Annexure 14, Guidelines for website audit:	Annexure 14 describes the processes to be followed when the web sites are to be hosted by the National Informatics Centre. Many of the sections in the annexure are not relevant to the current scope of work as the in-scope applications have already been hosted. Will it suffice if we demonstrate that our methodology and tools ensure the coverage of OWASP top ten? What sections of annexure 14 are relevant as per the scope of work?	**This is as per RFP.**
19	Clause 1.6 Award and Duration of the work:-> The successful bidder is expected to complete the work within a period of 180 days once the work has started:-	During the audit assignment, the auditor will identify bugs / vulnerabilities which then would be forwarded to the website vendor to resolve the issues. The vendor will take their own time on which auditor will not have any control. Any delay on part of website vendor in giving their revised delivery might result into some delay in the audit project period also. Due to this dependency of auditor on website vendor to resolve the issues, any time taken by the vendor to resolve the bugs is normally not counted in the stipulated 180 days.	**This is as per RFP.**
20	Section 1.3.2, subpoint (h), page 10 – The RFP states that "Bidder should have experience of conducting similar website audit as proposed by Department of Information Technology, Government of NCT of Delhi of a minimum of 3 audit projects in organizations like banks, financial institutions, Insurance companies or Government departments**.**	". Kindly, clarify is there is a specified time duration in which the bidder should have carried out these audits	**This is as per RFP.**

21	Section 1.12, Page 17 – The RFP states that "Successful bidder need to take the required permission from the particular department. The successful bidder will also conduct a conference with the respective department/ corporation/ local bodies.".	Considering that there are multiple department/ corporation/ local bodies, kindly clarifythat the responsibility of co-ordinating this meeting will be with DIT or with bidder? Also, will this be a single meeting or multiple meetings? If multiple meetings, then kindly let us know the anticipated number of meetings.	**The Department of IT will supplement efforts of the Bidder to co-ordinate with all the departments.**
22	Section 1.15, Page 18 – The RFP states that "The Auditor shall make good or compensate for, all direct damage occurring to website and web applications of the respective department and/or Department of Information Technology, Government of N.C.T of Delhi in connection with this Contract for carrying out audit. Provided that this Clause shall not apply if the Auditor is able to show that any such damage is caused or contributed to by the neglect or default of the respective Department. The security auditor's liability will be limited to the cost of service provided. Default or neglect by the Auditor will include both malicious and no malicious errors and project mismanagement.".	This clause is very restrictive and not favorable for the auditor, since the auditor will need to demonstrate that the damage, if any, is not due to the bidder. This may also result in the successful bidder not exploiting the weaknesses, since if it causes any damage then the auditor will be liable for it.	**The Department of IT will provide the backup of all the websites as mentioned in the RFP. The bidder has required to setup a staging server for audit of these websites .**
23	Section 1.24, Page 21 – The RFP states that "The Audit firm/company is required to follow-up with the concerned offices of the Department of Information Technology, Government of N.C.T. of Delhi and the concerned Department for compliance.".	Kindly clarify, that the responsibility of co-ordinating this meeting will be with DIT or with bidder? Also, will this be a single meeting or multiple meetings? If multiple meetings, then kindly let us know the anticipated number of meetings	**The Department of IT will supplement efforts of the Bidder to coordinate with all the departments.**
24	Section 1.24, Page 21 – The RFP states that "The Audit firm/company has to submit a summary compliance report at end of each task and the final report should be certify that the website/web applications (should be mentioned the name of the website and/or web applications) is "Certified for Security".	Kindly clarify, the expectation on security certified site/ application, since certification can be carried against a published and internationally recognized standard only. Also, Web site security audit only provides a reasonable assurance that the vulnerabilities have been identified and post implementation of recommendations, the gaps have been closed.	**This is as per RFP.**
25	Section 1.25, Page 21 – The RFP includes upon "Exit Plan in this section	". Kindly, clarify the expectation/ requirement of this section from the auditor.	**The Exit Plan has been mentioned in Clause No. 1.25 of RFP.**

26	Section 2.1.1, Page 23 – The RFP states that the "Auditor needs to check for various attacks – Phishing a website.	". Kindly clarify, the scope of the audit, since Phishing is carried out with the end-users and not on the infrastructure hosting web site/ application.	**The words "Phishing a website" in Clause No. 2.1.1, Task 1, Website Security Audit/Assessment stand deleted.**
27	Section 2.3, subsection 1, Page 26 – The RFP states that "Verification of possible vulnerable services will be done only with explicit written permission from the auditee." Also, the subsection 6 states that "Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering will be taken."	Kindly clarify, that auditor needs to take written permission from DIT or from individual department/ corporation/ local bodies? In case, multiple permissions are required, then please specify who will co-ordinate for getting this approval.	**This is as per RFP.**
28	Section 2.3, sub section 15, page 28 – The RFP states that "Reports should state clearly all states of security found and not only failed security measures.	." Kindly clarify the expectation on this, since audit reports are normally on exceptional basis and therby reporting only on exceptions noted.	**This is as per RFP.**
29		1) Approximate number of screens per site.	**This varies from website to website. The list of website is mentioned in RFP.**
30		2) Complexity of the function offered by web site. (high/medium/low)	**This varies from website to website. The list of website is mentioned in RFP.**
31		3) Whether user credentials will be shared or it will be black box testing.	**The credentials may be shared by the respective departments.**
32	Security deposit of Rs. 4,00,000 for the bid	Security deposit of Rs. 4,00,000 for the bid. Whetheher this requirement can be exempted for the Govt. of India deptt. Like us?	**Government departments are exempted for the security deposit.**
33	CISA/CISSP qualified professionals for conducting the audit.	You have asked for CISA/CISSP qualified professionals for conducting the audit. But our auditors do not possess the qualification. Instead we have experienced and qualified auditors with BS 7799 LA (Lead Assessor) and CEH (Certified Ethical Hacking) certifications. Please tell us whether this will satisfy the eligibility criteria.	**This is as per the RFP.**