

**Amendments & Clarifications for Request for Proposal for Supply and Maintenance of Application Security Testing Solution**
**Ref : CO:ITD:559/R1:2018-19 Dated 14/09/2018**
**Amendments**
**Date:03/10/2018**

SI No.	RFP Page no.	RFP Point no.	RFP Clause	Amended Clause
1	18	4.6.4	<p>The Solution should be able to integrate and scan following programming languages:</p> <p>a) .net technologies (C# , J# ,VB.net , ASP.net , .Net core etc)</p> <p>b) Java</p> <p>c) PHP</p> <p>d) ASP</p> <p>e) Python</p> <p>f) SQL, T-SQL ,PL/SQL</p> <p>g) HTML/HTML 5</p> <p>h) XML</p> <p>i) CSS</p> <p>j) JavaScript</p> <p>k) JQuery</p> <p>l) C</p> <p>m) C++</p> <p>n) COBOL</p> <p>o) Perl</p>	<p>The Solution should be able to integrate and scan following programming languages:</p> <p>a) .net technologies (C# , J# ,VB.net , ASP.net , .Net core etc)</p> <p>b) Java</p> <p>c) PHP</p> <p>d) ASP</p> <p>e) Python</p> <p>f) SQL, T-SQL ,PL/SQL</p> <p>g) HTML/HTML 5</p> <p>h) XML</p> <p>i) CSS</p> <p>j) JavaScript</p> <p>k) JQuery</p> <p>l) C</p> <p>m) C++</p>
2	22	4.7.6.6	<p>The solution should have the ability to Integrate with security information and event management (SIEM) system</p>	<p>Clause has been dropped</p>

SI No.	RFP Page no.	RFP Point no.	RFP Clause	Amended Clause
3	23	5.8 Qualification Criteria	The bidder should have implemented the solution in at least two (2) Scheduled Commercial Bank/National Informatics Center/Corporate in India in the last three years (i.e. from 1/1/2015 to 31/12/2017)	The bidder should have implemented the solution in at least two (2) Scheduled Commercial Bank/National Informatics Center/Corporate in India during the period from 1/1/2015 to 31/08/2018
4	41	19.3	The Bidder should be Net profit earning organization in the last three (3) financial years, i.e.(2015-16,2016-17 & 2017-18)	The Bidder should be Net profit earning organization in the last two (2) financial years, i.e.(2016-17 & 2017-18)
5	Not Available in RFP	4.7.1.22	New clause	The DAST solution should support Interactive Application Security Testing features
6	Not Available in RFP	4.7.1.23	New clause	The Solution Should have the capability to bypass captcha

### Clarifications

Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
1	16	4.1	Licenses required : Static application security testing (SAST) license -25 , Dynamic application security testing (DAST) license - 5	As per the tender Bidder will supply only the Software Licenses and Installation, Configuration and Commissioning of the licenses in the Bank. The required hardware and Supporting software will be provided by the bank. Request Bank to confirm.	It is clarified that Supporting Hardware will be provided by the bank. The successful bidder should provide all software with licenses except the Operating system.



Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
				Based on our experience with large PSU banks, we recommend the bank for 2 concurrent licenses. (Since it is concurrent no of users, software can be installed in multiple systems and scan can be done in 2 concurrent licenses.)	Please adhere to the RFP
2	17	4.4.8	Training is to be provided to Bank's employees for five (5) working days from OEM certified trainer. Training should cover on how to install the software in the IDE, how to scan the code, how to scan the application during the run time (DAST), how to generate the report, how to fix the vulnerabilities etc.	Request Bank to confirm on the number of participants.	The expected count of the members is 40.
3	17	4.5.3	The solution (SAST and DAST) should tightly integrate to each other in order to have control and visibility	Can you brief the expectation from IB here . So that we can Scope that.	It is clarified that the successful bidder should provide both SAST and DAST solutions in same environment and the code after testing in SAST, the DAST should provide runtime testing.
4	18	4.5.19	The software installation and configuration for the entire setup must be handled by the qualified/experienced OEM personnel only	Does this mean the OEM should do the installation - Please clarify?	OEM personnel to do the Installation. Please refer the point number 4.5.7
6	18	4.6.5	The solution should have integration capabilities which can be integrated in every phase of SDLC. The solution should be capable of integrating with source	Do you want the integration with IDE & build management from day one , or it's a features to be available & will be purchased when needed .	Integration with IDE is expected from Day One

Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
			code repository, IDE, Plug-in, build server, build management, bug tracking system and ticketing system. It should be able to integrate with the commercial or free IDEs (the list is not exhaustive rather only indicative) - a)Visual Studio 2015/17 b)Eclipse c)Android Studio		
7	21	4.7.4.2	The solution should have ability for determining code coverage completeness to understand and highlight areas of the application that were not covered with the testing	Request to remove as this is not applicable	It is clarified that if the code file is complete the SAST software should provide the information about the incomplete code.
8	22	4.7.7.3	The solution should verify compatibility while doing migration of source code across versions.	Please clarify if Bank is referring to the compatibility in terms of scanning source files at different point in time / functionality of application with different version.	Migration includes change in frame work , version of the programming languages etc
9	22	4.7.8.1	The solution should have the ability to perform testing on unlimited web applications within the same engine/installation	SAST is offered on number of developers based and DAST is offered based on number of Testers / Machines installed. Hope our understanding is correct and please confirm the same.	SAST is offered on number of developers based and DAST is offered based on number of Testers / Machines installed .
10	22	4.7.10	The solution must have a provision to provide the reports noted below. 4.7.10.1 Summary of support status 4.7.10.2 Significant incidents raised by the bank in the month. These include all priority observations and any other incidents reducing the quality of service. 4.7.10.3	While the offered solution doesn't offer automated reporting functionality of the mentioned reports, the same can be achieved manually by tracking the same.	Accepted. All reports should be available for pulling it from the system.



Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
			Number of support calls closed during the month, by priority 4.7.10.4 Number of support calls open at the end of the month, by priority 4.7.10.5 Patch, Fixes, update reports 4.7.10.6 Application bugs/Issue call analysis 4.7.10.7 Proactive monitoring and preventive maintenance report.		
11	23	5.4	The Annual turnover should be more than Rs.3 Crores in last three (3) financial years, i.e.(2015-16,2016-17 & 2017-18)	The balance sheet for 2017-18 is not ready yet. Can we submit the balance sheet for 2014-15 instead? or is it mandatory to submit 2017-18 in order to be eligible to participate in the tender?	Please adhere to the RFP
12	23	5.6	The Bidder should have a branch in Chennai.	Is this a mandatory requirement? what if one organization does not have a branch yet has a strong technical team to deliver and support the requirement?	Please adhere to the RFP
13	23	5.7	The bidder should have a team of well qualified and experienced staff, in bidder's Chennai branch, who will be able to attend the calls in person/provide onsite support, respond to the issues at a very short notice and they should have the knowledge to extend support to the bank for the in-scope activities on a need basis.	Is it ok if the bidder does not have qualified team based out of Chennai but in other places like Bangalore/ Mumbai etc?	Please adhere to the RFP



Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
14	23	5.8 Documents Required	The bidder must produce purchase order/ reference letter from their customer duly mentioning the solution name. The bidder should also furnish the details as per section 12.	Qualification Criteria: The bidder/ <b>OEM</b> should have implemented the solution in at least two (2) scheduled commercial bank/national informatics center/corporate in India in the last three years (i.e. from 1/1/2015 to 31/12/2017)	Please adhere to the RFP. Also refer Amendment-3 for qualification criteria.
15	41	19.8	The bidder should have implemented the solution in at least two (2) Scheduled Commercial Bank/National Informatics Center/Corporate in India in the last three years (i.e. from 1/1/2015 to 31/12/2017)	Any other application security is ok or should only be bidder proposed application security product	Please adhere to the RFP  Also refer Amendment-3 for qualification criteria.
16	NA	NA	NA	Will the application development team / initiate the scan from IDE or build Management ?	Development team will initiate the scan from IDE
17	NA	NA	NA	Hope the H/W requirement for implementation Server etc , will be provided by IB	Yes. The bidder need to provide the hardware requirement for the proposed software solution being quoted.
18	NA	NA	NA	Will there be a score for technical weightage given. As technically good products might not be L1 & the bank might end up in deciding on price .	No extra weightage is available
19	NA	NA	NA	Incremental scan capability to be available for all the languages with same specification mentioned	Incremental scan capability is not mandatory
20	NA	NA	NA	Open source libraries scanning to be included as part of the source code scanning	The solution has to provide the ability to scan the entire source code for vulnerabilities which may or may not include Open source libraries

Sl. No.	RFP Page No.	RFP Point No./Title	Details Provided in RFP	Query/Changes Requested	Banks Response
21	NA	NA	NA	Will the application development team / initiate the scan from IDE or build Management ?	Application team will initiate scan from IDE
22	NA	NA	NA	Hope the H/W requirement for implementation Server etc , will be provided by IB	The bidder to provide the hardware requirement
23	NA	NA	NA	Will there be a score for technical weightage given. As technically good products might not be L1 & the bank might end up in deciding on price .	No extra weightage is available
24	NA	NA	NA	is this the No. of Applications / projects ? Can you share the No. of users who will be using the tool ?	SAST license is based on number of developers

