RFP for "Cloud Based Web Application Firewall & DDoS Attack Protection Services" (*RFP No. NB.HO.DIT/1471/DIT-012-15/2019-20) dated 13 January 2020*

Reply to Pre-Bid Queries

S. No.	Page no. of RFP	RFP Clause No.	RFP Clause	Comment/Query/Suggestion/Modification	NABARD's Comment
1	16	2	WAF and DDoS protection services should be provided on Security-as-a-Service model.	Can both the services be provided as managed security service from the bidder SOC?	Yes
2	16	6	The Solution should support "On Demand" Vulnerability Scanning of Applications i.e. the solution must be able to integrate with web application vulnerability assessment tools.	Kindly mentioned the existing VAPT tool details or we have to provide VA & PT services separately. Please clarify if VA tools are also required. Please specify the web application vulnerability tool that you are referring to.	The bidder has to provide the services. The bidder has to arrange for any standard VA tool.
3	16	11	Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement	Requesting to modify the point as "Any new vulnerability discovered/disclosed publicly and acknowledged by NABARD should be included in the scan policy within 36 hours of announcement"	No change. The bidder/OEM will have to acknowledge the vulnerability depending on the advisories/publications issued by NCIIPC, CSITE, etc.
4	17	22	The solution should include options to generate scanning and vulnerability reports as and when required by the Bank.	Is there an expectation to WAF should have inbuilt capability for the scanning.	Yes.

5	17	25	The provided WAF service should be in Auto Scaling/High availability mode such that there will be no impact on WAF service delivery in case of downtime or other operational issues at bidder's side.	Need to amend as following: Need to amend as following: The provided WAF Service from OEM should be able to provide availability SLA of 99.999%	No change.
6	17	30	The WAF solution should have inter alia capability of protection from BOT and Man-in-The-Browser Attack. Administrators must be alerted through mail/SMS in case of such attack."	**Need to amend as following:** The OEM should forward all the attack information to the customer for the BOT and Man-in-the-Browser Attack; on E Mail	No change.
7	18	3.2	Commercial Evaluation		Refer to corrigendum .
8	19	5	The solutions for identified vulnerabilities by way of vulnerability assessment done should be provided within 24 hours for Critical vulnerabilities. For all other vulnerabilities, solution should be provided within a maximum of 72 hours. In case of failure to do so, a penalty of 5% of Quarterly Costs will be charged for every 24 hours' delay, subject to a maximum of 10% of the Cost per quarter.	We assume that here we are refering to solution provided on which we have to fix the vulnerability. Also we request you to consider only response time as we there may be a time where we are dependent on OEM to release patch/upgrades/updates to fix the vulnerabilities.	No change.
9	22	3	WAF for the applications should be deployed within 15 days of issue of Purchase Order.	Requesting you to increase the implementation timeline	Refer to corrigendum.

10	22	4	The Signing of contract should also be completed within 7 days of Purchase Order.	Requesting you to increase the contract signing timeline	No change.
11	23	3(iii)	There sje Daily report on the performance of the WAF.	Typo Error.	Refer to Corrigendum.
12	52	3	The bidder should have at least 3 successful implementations of the WAF solution of which 1 should be in the BFSI sector	We request you to change from Bidder or OEM. Due to WAF on Cloud many installation is not done by many partner's and customer …Having this clause many of vendor will have opportunity to quote	No change. For bidder, the cloud based WAF implementation is not a prerequisite. Both on-prem & cloud based WAF implementations will be accepted.
13	53	5	The OEM should possess ISO 27000 series certifications.	OEM has implemented ISO 9001. Requesting to relax the requirement for ISO 27000 series certifications.	Refer to Corrigendum.
14	53	5	The OEM should possess ISO 27000 series certifications.	Since this services are leveraged banking use, only ISO 27017 certification is not enough to regulate security and compliance of Cloud Vendors, there are many other certification which are required for Security Cloud OEM to follow with below certifications as well - PCI-DSS - The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information	Refer to Corrigendum.

				- SOC 1 type 2 - Includes the design and testing of controls to report on the operational effectiveness of controls over a period of time (typically six months) - SOC 2 Type 2 - Service organizations that hold, store or process information of their clients, these certification ensures its system is designed to keep its clients' sensitive data secure - Both SOC 1 Type 2 and SOC 2 Type 2 are required to ensure data is secure "The service provider should possess ISO 27017, 28000 ; SOC 1 Type 2 and SOC 2 Type 2 certification"	
15	53	7	The OEM should have at least 3 successful implementation of Cloud based Web Application Firewall in BFSI sector.	Requesting concession on turnover and experience for Bidder and OEM as per Govt. of India tender guidelines for Start-ups.	Refer to Corrigendum.
16	59	7	After patching the identified vulnerabilities, a final targeted scanning for those specific vulnerabilities should be carried out.	Please elaborate on this.	It's just the reassessment of patched vulnerabilities.
17	59	13	The WAF should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic.	Current TLS standards are on TLS1.3 with support for ECC standards, **Clarification:** Do we need Cloud WAF to be compatible with such latest TLS standards **Amendments:** The WAF should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic with all latest standards to include TLS1.3 with EC-P256 standards but limited to it.	No change.

18	60	16	The WAF should support millisecond latency so as not to impact Web application performance.	Please clarify on this. Also, please let us know the location of DC & DR where the servers, applications are hosted	Currently DC is in Mumbai and DR is in Faridabad.
19	79	2.1.2	The SI should provide a Technical Account Manager (TAM) support for at least 03 months from the date of acceptance of Solution, from OEM of the solution.	Please list the scope of work of the TAM.	No change. Already included in the RFP.
20	80	2.2.2	M/s _____shall provide training at NABARD Head Office, Mumbai or any other location as specified by Bank to the number of personnel identified by the Bank on functional, operational and reporting aspects of the Proxy solution. The training material will also have to be provided in English.	Kindly quantify the number of personnel to be trained, location of training and wether NABARD will be liable for expenses if training is conducted at partner location.	Refer to Corrigendum
21			Additional Point	Should have Unified Portal for WAF and DDoS	Refer to Corrigendum
22			Additional Point	No hardware & software is to be installed at Bank premises for the provision of the services.	Already included in the RFP.

23			Additional Point	Cloud WAF solution should be Full PCI Compliance with all 10 security mechanisms of PCI-DSS Requirement 6.6, including enforcing a positive security model and implementing data leakage prevention (DLP) controls	No change.
24			Additional Point	Should be able to provide User Defined Customized Reporting	Refer to Corrigendum
25			Additional Point	Should be able to provide Compliance Reporting	Refer to Corrigendum
26			Additional Point	Should not have any restriction on no. of Rules	Refer to Corrigendum
27			Additional Point	Should provide complete managed Services - Configuration, Operations and Management	Refer to Corrigendum
28			Additional Point	Should provide capability to configure Custom Rules	Already included in the RFP.

29			Additional Point	The scanning reports should have no false positives and provision for exception to review and resolve the same, if any.	Already included in the RFP.
30			Additional Point	Should have option to upgrade solution with full fledged BOT Management solution in future on-demand with below capabilities	No change.
31			Additional Point	Defend against bots that target digital assets, including sophisticated bots designed to hit multiple assets	No change.
32			Additional Point	Detect and identify bots using a multi-layered approach, including signatures of known bots, HTTP profiling, device fingerprinting, CAPTCHA, Behavioral challenges and semi-supervised machine learning	No change.
33			Additional Point	Detect and block sophisticated humanlike bots in real time with no impact on the technology stack	No change.
34			Additional Point	Identify the intent of bots with the highest precision through proprietary, semi-supervised machine learning models	No change.

35			Additional Point	Cloud WAF should provide Application Analytics	No change.
36			Additional Point	Cloud WAF Application Analytics must consolidates large number of similar events into manageable sets of recurring activities to effectively handle	No change.
37			Additional Point	Security events provided should have context on application behaviour and why certain events are blocked or allowed, displaying key activity details such as recurrence and usage trends over time	No change.
38			Additional Point	Cloud WAF Portal should provide drill-down about security events and patterns, including context & clarify into application behaviour like Attack details, HTTP request, Vulnerabilities, origin country of attacker, OWASP Category of attack event falls into and many more.	Refer to Corrigendum
39			Additional Point	Should be able to perform SSL/TLS Enforcements	Already included in the RFP.
40			Additional Point	Should have Geo-IP Blocking capability	Already included in the RFP.

41			Additional Point	Should provide DDoS protection of up to 1Gbps and option to upgrade DDoS attack mitigation to unlimited	No change.
42			Additional Point	Service should provide Portal Access and for Multiple People with different level of Privileges.	Refer to Corrigendum
43			Additional Point	Should be able to protect based on Behavioral network- and application-layer DDoS protection with network challenge-response	No change.
44			Additional Point	Should be PCI-DSS Certified	No change.
45			Additional Point	Should be GDPR Compliant	No change.
46			Additional Point	Should be OHSAS Certified	No change.

47			Additional Point	Please let us know the number of applications to be considered for WAF	Currently the no. of applications is 10, In future it can increase to 30 (up to next 3 years.)
48			Additional Point	Please let us know the web application throughput that needs to be considered	100 Mbps is already mentioned in the Commercial Bid Form.
49			Additional Point	Can we propose different OEM for WAF & DDOS	Yes, but there should be a unified console.
50			Additional Point	Do you have an public IP pool of your own or provided by service provider	Public IPs are provided by service provider.

----------End of Document----------