**Corrigendum to the 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***

| S. No. | RFP Page No. | Clause No. / Clause Pertaining to | RFP Clause | Revised Clause |
|---|---|---|---|---|
| 1 | 7, 63 | Commercial Bid Form | Commercial Bid Form | Please see the Annexure -1 on Revised Commercial Bid Form. |
| 2 | 22 | 5.1.3 | WAF for the applications … | The applications should be on-boarded on the WAF & DDoS solution within 15 working days of the issue of Purchase Order. The WAF solution should be brought in mitigation mode within next 15 working days. |
| 3 | 23 | 3(iii) | There sje Daily report …. | There should be facility of generating daily report in the console, on the performance of the WAF & DDoS protection solution. |
| 4 | 53 | 5 | The OEM should possess …… | The service provider should possess ISO 27017, 28000 ; SOC 1 Type 2 and SOC 2 Type 2 certification. |
| 5 | 53 | 7 | The OEM should have at least 3 successful……. | The OEM should have at least 3 successful implementation of Cloud based WAF, of which at least 1 should be in BFSI sector. |
| 6 | 53 | 7 | The format for certificate, to be ……. | The format for certificate, to be submitted, is provided in Annexure-I. Necessary documents (Like PO) should be attached.<br>Email confirmation from the customer, directly sent to dit@nabard.org, confirming the implementation, may also be arranged. Contact details of the customer will also have to be shared with NABARD. |
| 7 | 78 | SLA | "M/s_____, a company incorporated under the provisions of the Companies Act,……. | M/s_____, a company incorporated under the provisions of the Companies Act, 1956 and having its registered office at _____, together with its Affiliates and represented herein by its Authorised Signatory, _____hereinafter referred to as "M/s_____", (which expression shall mean and unless repugnant to the context, includes its successors in business, legal representatives and administrators or permitted assigns) of OTHER PART." |

| | | | | |
|---|---|---|---|---|
| 8 | 80 | 2.1.3 | The SI onsite engineer, along with the TAM of the OEM shall do……. | The SI onsite engineer, along with the TAM of the OEM shall do a "knowledge transfer" to the identified officers of NABARD and engineers of our IT services management vendor during the last month of support to ensure smooth takeover of the operations and management of the **Cloud based WAF & DDoS Attack Protection** |
| 9 | 80 | 2.2.2 | M/s _____shall provide training at NABARD Head Office, Mumbai or any other location as….. | 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 **Cloud Based WAF & DDoS Attack Protection** solution. The training material will also have to be provided in English. The cost may be factored in the support cost in the Commercial Bid Form. |
| 10 | 93 | 2.1.3 | The SI onsite engineer, along with the TAM of the OEM shall do……. | The SI onsite engineer, along with the TAM of the OEM shall do a "knowledge transfer" to the identified officers of NABARD and engineers of our IT services management vendor during the last month of support to ensure smooth takeover of the operations and management of the **Cloud based WAF & DDoS Attack Protection** |

**<u>Modifications in Annexure – L (Technical Bid Form)</u>**
**Following mandatory technical parameters are being added at Page no. 61, S. No. 32 onwards**

| S. No. | Page No. | RFP Clause No. | Added Technical Parameter | Remarks |
|---|---|---|---|---|
| 1 | 61 | 32 | Should have a Portal for WAF and DDoS protection solution, preferably unified. | Please see the Annexure-2 on Revised ***Technical Bid Form***. |
| 2 | | 33 | Should be able to provide User Defined Customized Reporting | |
| 3 | | 34 | Should be able to provide Compliance Reporting | |
| 4 | | 35 | Should not have any restriction on no. of Rules | |
| 5 | | 36 | Should provide complete managed Services - Configuration, Operations and Management | |
| 6 | | 37 | Cloud WAF Portal should provide drill-down about security events and patterns, including context & clarify Attack details. | |
| 7 | | 38 | Service should provide Portal Access for Multiple People with different level of Privileges. | |

**ANNEXURE -1**

**Annexure - N**
**Commercial Bid Form**

| Sr. No. | Requirement | Cost Details Per Annum | | | Cost for 03 years (4) (Rs.) |
|---|---|---|---|---|---|
| | | Cost (1) (Rs.) | GST (2) (Rs.) | Total Cost (3) (Rs.) | |
| **A.** | Cost of the Solution for **Clean Throughput** of minimum 50 Mbps | | | | |
| **B** | Support Cost (If any) | | | | |
| **C** | One-time Implementation Cost (If any) | | | | |
| **D** | **Total Cost (A+B+C)** | | | | |
| **E** | **Incremental Cost:** (Additional **Clean** Throughput of 5 Mbps) | | | | |
| | Calculation of TCO based on estimated requirement of **Clean** Throughput of **100** Mbps | **TCO = 4D + (4E*10)** | | | |

**Instructions:**

1. The application may be web or mobile.
2. NABARD would be free to host any number of applications, subject to the throughput and data transfer limits.
3. The Incremental cost will be valid till the entire contract period including extensions thereof.
4. The training cost, if any, will have to be covered under Support Cost.
5. The TCO for identifying L1 bidder would be the cost for 100 Mbps **clean** throughput (including 50 Mbps incremental throughput). Order will be placed on actual requirement as and when it arises.
6. In calculating the Commercial Evaluation, commercial bids of technically qualified short-listed bidders will only be opened.
7. Any change/deviation in bid which has bearing on commercials will not be entertained.
8. NABARD reserves the right to rectify any minor arithmetic errors in the commercial bid and bidder is bound to accept the same.
9. There should be no limit on monthly data transfer.

**Name and Signature of the Bidder:**

**Business Address:**

**Date:** **Place:**

## ANNEXURE -2

### Annexure - L
### Technical Bid Form

**All Technical Parameters, mentioned below, are mandatory.**

| Sl. | Description | Compliance (Yes/No) | Bidder Remarks |
|---|---|---|---|
| 1 | All Internet traffic meant for the Bank's web facing applications that are integrated in WAF shall be routed first to the WAF on the cloud for scanning & only genuine traffic shall be forwarded to the Bank's application. | | |
| 2 | WAF and DDoS protection services should be provided on Security-as-a-Service model. | | |
| 3 | The service should be comprehensive and should include Configuration, Operations and Management of the solution. | | |
| 4 | No hardware & software is to be installed at Bank premises for the provision of the services | | |
| 5 | WAF shall ensure automatic protection with minimum manual intervention for initial configuration, timely policy updates, and others operational activities as required. | | |
| 6 | The Solution should support on demand Vulnerability Scanning of the Application i.e. the solution must be able to integrate with web application vulnerability assessment tools. | | |
| 7 | After patching the identified vulnerabilities, a final targeted scanning for those specific vulnerabilities should be carried out. | | |
| 8 | The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities, SANS Top 25 Vulnerabilities and WASC Web Security Attack classification. | | |
| 9 | It should be able to prevent all application security threats including Cross Site Scripting (XSS), SQL injection, remote file inclusion, Brute Force Attack, Buffer overflow, Cookie poisoning & Cookie Protection and Parameter tampering. | | |
| 10 | The solution should support both Positive and Negative security models | | |
| 11 | The solution should provide full support for HTML5, AJAX and JSON. | | |
| 12 | Any new vulnerability discovered/disclosed publicly should be included in the scan policy within 36 hours of announcement. | | |

| | | | |
|---|---|---|---|
| **13** | The WAF should be capable of decrypting the SSL/TLS traffic to analyse the HTTP data, and re-encrypt the SSL/TLS traffic. | | |
| **14** | WAF should support different policies for different web applications, and allow modification of these policies upon request. | | |
| **15** | The solution should include options to develop unlimited Custom Rules, Proof of Concepts and Virtual Patching for detected vulnerabilities. | | |
| **16** | The WAF should support millisecond latency so as not to impact Web application performance. | | |
| **17** | The plan should include clean or legit data transfer of 500GB per month for all applications put together. | | |
| **18** | WAF should be able to handle throughput with scalability of handling https traffic up to 50 Mbps. | | |
| **19** | The WAF must be able to secure & protect web, mobile, and API applications on request." | | |
| **20** | On request integration of new applications, increase in data transfer and throughput should be provided at quoted rates. | | |
| **21** | The WAF should allow for exception handling like Whitelisting and Blacklisting of IPs, and allow blocking of IPs based on geographic location. | | |
| **22** | WAF should provide a real-time single management console to manage multiple WAF instances protecting multiple websites. The dashboard should contain data such as top attacks view, traffic monitoring view, etc. | | |
| **23** | The solution should include options to generate scanning and vulnerability reports as and when required by the Bank. | | |
| **24** | Once the vendor patches the identified vulnerabilities, a final targeted scanning for those specific vulnerabilities must be carried out under advice to the Bank. | | |
| **25** | The scanning reports should have minimum false positives and provision for exception to review and resolve the same, if any. | | |
| **26** | 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 | | |
| **27** | The DDoS solution should protect against emergent DDoS attack vectors such as Dynamic IP, Pulse, Burst DDoS attacks and other zero-day attack methods. | | |
| **28** | The DDoS solution should provide protection against Layer 3, 4 volumetric attacks and Layer 7 DDoS attacks. | | |

| | | | |
|---|---|---|---|
| **29** | WAF and DDoS should be from same OEM so that there is a tight integration between both in terms of integration and security | | |
| **30** | The solutions provided should have SIEM integration capability. | | |
| **31** | 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. | | |
| **32** | Should have a Portal for WAF and DDoS protection solution, preferably unified. | | |
| **33** | Should be able to provide User Defined Customized Reporting | | |
| **34** | Should be able to provide Compliance Reporting | | |
| **35** | Should not have any restriction on no. of Rules | | |
| **36** | Should provide complete managed Services - Configuration, Operations and Management | | |
| **37** | Cloud WAF Portal should provide drill-down about security events and patterns, including context & clarify Attack details. | | |
| **38** | Service should provide Portal Access for Multiple People with different level of Privileges. | | |

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