Amendment-1 to "RFP 32/2017-18 dated 07/02/2018 for Supply, Installation, Integration, Provisioning, Commissioning, Monitoring, Maintenance and Support for Internet Links with Secure DDOS Protection Solution"

It is decided to amend the following in respect of the above RFP:

Sl. No.	Page No.	Clause No.	Existing	Amended
a.	9	8. Requirement Details:	8.2 We have requirement of comprehensive solution for below mentioned services: 8.2.1 Dedicated 100 mbps and 50 Mbps Full duplex Internet Bandwidth with dual last mile connectivity at Bank DC and DRC. 8.2.2 IPv4 and IPv6 Public IP from service provider. 8.2.3 Managed Network Services for conversion of IPv6 protocol to IPv4. 8.2.4 Cloud based Volumetric DDOS Protection	8.2 We have requirement of comprehensive solution for below mentioned services: 8.2.1 Dedicated 100 mbps and 50 Mbps Full duplex Internet Bandwidth with dual last mile connectivity at Bank DC and DRC. 8.2.2 IPv4 and IPv6 Public IP from service provider. 8.2.3 Managed Network Services for conversion of IPv6 protocol to IPv4. 8.2.4 **Cloud based Volumetric DDOS Protection from ISP's own scrubbing centre (ONNET)**
b.	9	8. Requirement Details:	8.4. The Bank reserve the right to continue/renew/terminate any of the above services at the discretion of the Bank and shall terminate the services by giving 30 days notice period to the bidder.	**8.4.** The Bank reserve the right to continue/renew/terminate any of the above services at the discretion of the Bank and shall terminate the services by giving 30 days notice period to the bidder. **However, for Internet Link services a notice period of 60 will be provided to the selected Bidder.**
c.	11	9. Scope of Work:	9.24. Anti-DDoS solution Service provider must provide alert within 5 minutes of detecting DDoS attack.	**9.24.** Anti-DDoS solution Service provider must provide alert within **15 minutes** of detecting DDoS attack.
d.	11	9. Scope of Work:	9.29. The solution should have capability to generate Alerts and Logs that DDoS attack has been detected. The bidder must also notify the Bank in timely manner through Call, SMS on mobile and through E-mail to the registered credentials of the concerned Bank official when any DDoS attack is detected.	**9.29.** The solution should have capability to generate Alerts and Logs that DDoS attack has been detected. The bidder must also notify the Bank in timely manner through Call and E-mail to the registered credentials of the concerned Bank official when any DDoS attack is detected.
e.	13	9. Scope of Work:	9.35. Provision of the link is subject to satisfactory Acceptance Test. The bidder shall arrange for the UAT and required tools as per Bank's requirements. After commissioning the links,	**9.35.** Provision of the link is subject to satisfactory Acceptance Test. The bidder shall arrange for the UAT and required tools as per Bank's requirements. After commissioning the links,

			Acceptance Test will be finalized after observing the links for 30 days. The methodology for the test will be at the discretion of Bank. The link commissioning is deemed to be complete only if the acceptance test results are found satisfactory. Acceptance tests will be conducted by the Bank at its premises at Mumbai & Bangalore.	Acceptance Test (performance parameter e.g. latency, reliability, jitter etc.) will be finalized after observing the links for 7 days. The methodology for the test will be at the discretion of Bank. The link commissioning is deemed to be complete only if the acceptance test results are found satisfactory. Acceptance tests will be conducted by the Bank at its premises at Mumbai & Bangalore.
f.	29	45. Penalties/ Liquidated Damages:	**45.2. Penalties/Liquidated damages for onsite resources:** In case the resources goes on leave/absent, replacements having equivalent or more experience and qualification has to be arranged by the Bidder to ensure that regular functioning of the branch/office does not hamper. In case replacements are not arranged, bank shall pay only the proportionate amount of Resident resource charges during the particular quarter. The Bank shall also impose a penalty of 0.5% (Plus GST) of the Resident resource charges (Excl. of Taxes) payable to the Bidder for that quarter for each week and part thereof of absence. However, total penalty under this clause will be limited to 20% (Plus GST) of the total charges (Exclusive of Taxes) payable for Resident Resource charges for that quarter.	The RFP clause stands deleted.
g.	30	47. Payment Terms	47.1. Payment schedule will be as under: a. Link Charges-100%-Payment will be quarterly basis after deducting applicable penalties and Liquidated damages.	47.1. Payment schedule will be as under: a. Link Charges-100%-Payment will be quarterly basis in arrears after deducting applicable penalties and Liquidated damages.
h.	32	49. Support:	**49.6. Response Time and Meantime to Restore [MTTR]** 49.6.1. Response Time and Meantime to Restore [MTTR] **49.6.2. Response Time shall be 5 minutes for DDOS attack alert and less than equal to 30 Minutes for other services and MTTR shall be 2 hours. Time specified above is from lodging of complaint.**	**49.6. Response Time and Meantime to Restore [MTTR]** 49.6.1. Response Time and Meantime to Restore [MTTR] **49.6.2.** Response Time shall be 15 minutes for both DDoS attack alert (detection & alert) & mitigation-post confirmation from Bank. Response Time less than or equal to 30 minutes for all other services as per RFP/Agreement/Contract and MTTR shall be 2 hours.

i.	44	Annexure-3 Eligibility Criteria Declaration Criteria no. b	<u>Eligibility Criteria:</u> The bidder/ISP must be a Tier - I provider and Category-A (class-A) ISP license holder from DoT, Government of India. <u>Documents to be submitted:</u> Bidder has to provide self-certified letter for Tier - 1 provider. Bidder has to necessary documents from DoT, Government of India for Cat-A ISP license holder.	<u>Eligibility Criteria:</u> The bidder/ISP must be a Tier-1/Tier-2 ISP (Internet Service Provider) and holding Category-A (class-A) ISP license from DoT, Government of India. <u>Documents to be submitted:</u> Bidder has to provide self-certified letter for Tier-1/Tier-2 ISP. In case of Tier-2 ISP, submit the following documents - i) network diagram depicting multi-homed Tier-1 ISPs connectivity & Internet Gateways. ii) declaration from the bidder that they will maintain multi-homed connectivity with Tier 1-ISPs for full contract period as per this RFP. Bidder has to submit necessary documents from DoT, Government of India for Cat-A ISP license holder.
j.	44	Annexure-3 Eligibility Criteria Declaration Criteria no. d	<u>Eligibility Criteria:</u> The ISP should have its own International Internet Gateway. <u>Documents to be submitted:</u> The Bidder has to provide the necessary document from DoT, Government of India.	The eligibility Criteria stands deleted.
k.	54	Annexure-10 Technical Requirements for Internet Links with Secure DDOS Protection Solution	<u>A. Specification of Internet Link</u> **16.** The bidder must have the capacity to increase and decrease the bandwidth on demand and such changes in bandwidth must be provisioned within 7 days.	<u>A. Specification of Internet Link:</u> **16.** The bidder must have the capacity to increase and decrease the bandwidth on demand and such changes in bandwidth must be provisioned within 7 days on own Last Mile and other party Last Mile. In case the network equipments supplied at bank end does not support such increase then the same must be provisioned with 4 weeks for own Last Mile and 6 weeks time on other party Last Mile
l.	55	Annexure-10 Technical Requirements for Internet Links with Secure DDOS Protection Solution	B. <u>Managed Network Service Conversion of IPv6 protocol to IPv4:</u> **3.** The bidder/ISP should share the firewall and IPS services and should enable standard policies for IPv6 protocol for both Bangalore and Mumbai. (Prevention of DDOS attacks, Prevention of network reconnaissance and attacks, Prevention of IPv6/IPv4 address	B. <u>Managed Network Service Conversion of IPv6 protocol to IPv4:</u> **3.** The bidder/ISP should ensure network security for Bank's IPv4 & IPv6 traffic by deploying suitable network security devices at their infrastructure (e.g. firewall, IPS etc.) and should enable standard policies for IPv4 & IPv6 protocol (Prevention of DDOS attacks,

			spoofing etc.) For the entire Internet traffic towards Bank network.	Prevention of network reconnaissance and attacks, Prevention of IPv6/IPv4 address spoofing etc.) for both Bangalore and Mumbai location
m.	55	Annexure-10 Technical Requirements for Internet Links with Secure DDOS Protection Solution	**B. Managed Network Service Conversion of IPv6 protocol to IPv4:** 5. The bidder should ensure reachability of IPv6 resources through Bank Mumbai office also.	The RFP clause stands deleted.
n.	55	Annexure-10 Technical Requirements for Internet Links with Secure DDOS Protection Solution	**C. ANTI-DDOS SOLUTION: Specification for Cloud Based Volumetric DDOS Protection(Scrubbing) Solution:** 4. The proposed cloud mitigation services provider must mitigate attacks originated within India locally inside the country. The primary Scrubbing center as well as Backup center should be in India. Bank Public IP must not be advertised outside the country to divert the legitimate traffic beyond the borders of the country.	**C. ANTI-DDOS SOLUTION: Specification for Cloud Based Volumetric DDOS Protection(Scrubbing) Solution:** 4. The proposed cloud mitigation service provider must mitigate the attack at the origin or from the nearest scrubbing centre. The ISP (bidder) should have their own scrubbing centre in India. Bank's own public IPs or public IPs allotted for Bank's use (by bidder) must not be advertised outside India to divert the legitimate traffic beyond the borders of the country.
o.	55	Annexure-10 Technical Requirements for Internet Links with Secure DDOS Protection Solution C. ANTI-DDOS SOLUTION: Specification for Cloud Based Volumetric DDOS Protection(Scrubbing) Solution	Additional Technical Requirement as point no.26	26. Deterioration in the Service during DDoS attack mitigation should not be more than 10% from the required service parameters as specified in Annexure 10.A.a.7, 10.A.a.8, 10.A.a.9 and throughput requirement. Legitimate users should be able to access Bank's application through Internet without any hindrance during DDoS attack mitigation

All the other Instructions and Terms & Conditions of the above RFP remain unchanged.
Please take note of the above Amendments while submitting your response to the subject RFP.

Date: 26/02/2018
Place: Bengaluru

Deputy General Manager