RfP No. 500/2021/1615/CBO/ITV dated February 23, 2021

Pre-bid clarifications

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
1	Clause 6.1.1.7	18	ISP should have their OWN International Gateway in India, for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite)	Pls consider: ISP should have its own/direct/Leased access to International Gateway in India, , for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite)	**Change:** The Clause stands modified as under: ISP should have their OWN / Leased / direct International Gateway in India, for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite)
2	Eligibility Criteria point no. 4	50	ISP should have their OWN international gateway in India, for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite).	we request you to please remove this clause or amend this clause as: ISP should have their OWN / LEASED / Direct access to international gateway in India, for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite). Justification: This industry works on collaboration. It will not impact on any functionality or performance of the Internet leased line link. Moreover other Technical terms Link Latency, Packer Loss, Etc. has been so stringent to deviate as we are complying. Therefore it (Direct access clause) doesn't require	**Change:** The Clause stands modified as under: ISP should have their OWN / Leased / direct International Gateway in India, for providing Internet bandwidth, which should be connected onto international fiber systems only (not on satellite)
3	Eligibility Criteria point no. 6	50	The bidder must possess valid certification such as TL 9001 & ISO 27001.	We request you to please remove the TL 9001 certification. Justification: We request you to please remove the TL 9001 certification and consider the ISO 9001 for quality management and 27001 for Information security management certification.	**Change:** The Clause stands modified as under: The bidder must possess valid certification such as TL 9001/ISO 9001 & ISO 27001.
4	Clause 5.1.4	12	Last mile connectivity between banks locations and their local POP or exchange using their own infrastructure i.e. bidder should not hire last mile from another service provider	Consideration of hiring of last mile infrastructure	**Change:** The Clause stands modified as under: The bidder can hire last mile from third party service provider and should not be from existing Internet service provider of SIDBI. However, maintaining SLAs and service deliveries are responsibility of the bidder.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
5	5.8.7	16	. Non submission of feasibility report and / or carrying out of shifting / commissioning of links at new location as per schedule mentioned above will attract LD as specified in Section 10.3 of RfP.	If bidder is not feasible on new location, so bidder request SIDBI to allow bidder to provide lastmile on 3rd party on new location	**Change:** The Clause stands modified as under: The bidder can hire last mile from third party service provider and should not be from existing Internet service provider of SIDBI.. However, maintaining SLAs and service deliveries are responsibility of the bidder.
6	10.3.3	34	b) Uptime (%) Per Month Penalty Committed SLA >=99.5% Nil >= 98.5 and < 99.5 10% of monthly BW charges >= 97.5 and <98.5 20% of monthly BW charges >= 96.5 and < 97.5 30% of monthly BW charges >= 95.5 and < 96.5 40% of monthly BW charges >= 94.5 and < 95.5 50% of monthly BW charges < 95.5% 75% of monthly BW charges	Bidder request SIDBI to amend this clause as : Uptime (%) Per Month Penalty Committed SLA >=99.5% Nil >= 98.5 and < 99.5 2% of monthly BW charges >= 97.5 and <98.5 3% of monthly BW charges >= 96.5 and < 97.5 5% of monthly BW charges >= 95.5 and < 96.5 7% of monthly BW charges >= 94.5 and < 95.5 10% of monthly BW charges < 95.5% 15% of monthly BW charges	**Change:** The Clause stands modified as under: b) Uptime (%) Per Month Penalty Committed SLA >=99.5% Nil >= 98.5 and < 99.5 5% of monthly BW charges >= 97.5 and <98.5 10% of monthly BW charges >= 96.5 and < 97.5 15% of monthly BW charges >= 95.5 and < 96.5 20% of monthly BW charges >= 94.5 and < 95.5 25% of monthly BW charges < 95.5% 30% of monthly BW charges
7	Clause 10.3.3 b)	34	Availability / Uptime	Pls review penalty terms (as penalty is on higher side)	**Change:** The Clause stands modified as under: b) Uptime (%) Per Month Penalty Committed SLA >=99.5% Nil >= 98.5 and < 99.5 5% of monthly BW charges >= 97.5 and <98.5 10% of monthly BW charges >= 96.5 and < 97.5 15% of monthly BW charges >= 95.5 and < 96.5 20% of monthly BW charges >= 94.5 and < 95.5 25% of monthly BW charges < 95.5% 30% of monthly BW charges
8	9.1.2	30	6 Packet Loss/Drop <<<1 out of every one million packets	Bidder request amend this clause and packet drop/Loss to be is <1% and the same will be monitor between customer end to provider end router	Packet loss/drop - 1 out of every 1000 packets".
9	9.1.2	30	11 Online portal for bandwidth utilization, link performance etc. • Real Time, Hourly, Daily, Weekly and Monthly	Bidder request to amend this clause as : " Online portal for bandwidth utilization, link performance etc. • Near to Real Time, Hourly, Daily, Weekly and Monthly"	**Change:** The Clause stands modified as under: Real time may be read as near real time with delta less than 15 minutes.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
10	Service level agreement, Point 6	31	Packet loss/Drop - 1 out of every one million packets	Industry standard SLA for Leased line Internet Packet delivery is 99%. Request department to amend the same.	Packet loss/drop - 1 out of every 1000 packets".
11	5.6.3	15	. The bidder to carry out up-gradation of bandwidth within TWO WEEKS and de-gradation within ONE WEEK from the date of issue of PO / intimation	Bidder request SIDBI to increase the up gradation of bandwidth timeline from 2 weeks to 4 weeks	**Change:** The Clause stands modified as under: The bidder to carry out up-gradation of bandwidth within FOUR WEEKS and de-gradation within TWO WEEK from the date of issue of PO / intimation.
12	Clause 5.8.5	15	The bidder has to commission the links at new location within 4 WEEKS from the date of purchase order	Pls consider 8 weeks	**Change:** The Clause stands modified as under: The bidder has to commission the links at new location within 6 WEEKS from the date of purchase order
13	5.8.5	16	. The bidder has to commission the links at new location within 4 WEEKS from the date of purchase order	Bidder request SIDBI to increase the commissioning of links at new location within 8 weeks from the date of PO	**Change:** The Clause stands modified as under: The Bidder should deliver and commission the links including Router within SIX WEEKS FROM THE DATE OF PURCHASE ORDER / LOI.
14	5.8.5	16	The bidder has to commission the links at new location within 4 WEEKS from the date of purchase order.	Vendor request SIDBI to kindly change the commission timeline of link at new location from 4 weeks to 8 weeks.	**Change:** The Clause stands modified as under: The bidder has to commission the links at new location within 6 WEEKS from the date of purchase order
15	9.1.2	30	12 Up-gradation and de-gradation of bandwidth >>> Up-gradation - two weeks from date of Purchase Order	Bidder request to increase the up gradation of bandwidth from 2 weeks to 4 weeks	**Change:** The Clause stands modified as under: The bidder to carry out up-gradation of bandwidth within FOUR WEEKS and de-gradation within TWO WEEK from the date of issue of PO / intimation.
16	9.1.2	30	13 Up-gradation of DDoS capacity >>> 24 hours from date of Purchase order.	Bidder request SIDBI to increase the up gradation of DDoS capacity timeline from 24 hours to 7 days	**Change:** The Clause stands modified as under: The bidder has to carry out up-gradation / de-gradation of scrubbing capacity within 48 HOURS from the date of placing order / intimation.
17	Clause 9.1.2.12	30	Up-gradation and degradation of bandwidth	Pls consider 4 weeks for up-gradation	**Change:** The Clause stands modified as under: The bidder to carry out up-gradation of bandwidth within FOUR WEEKS and de-gradation within TWO WEEK from the date of issue of PO / intimation.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
18	Clause 9.1.2.13	30	Up-gradation of DDoS capacity	Pls consider 72 hours	**Change:** The Clause stands modified as under: The bidder has to carry out up-gradation / de-gradation of scrubbing capacity within 48 HOURS from the date of placing order / intimation.
19	Clause 9.1.2.14	30	Shifting of links	Pls consider 3 weeks for feasibility and 8 weeks for shifting	**Change:** The Clause stands modified as under: The bidder has to commission the links at new location within 6 WEEKS from the date of purchase order.
20	10.3.1	33	1. The bidder should undertake to commission the link / services / Router as per SoW within FOUR WEEKS from the date of purchase order / letter of Intent	Bidder request SIDBI to increase the delivery timeline from 4 weeks to 10 weeks as due to pandemic condition there is delay from OEM end	**Change:** The Clause stands modified as under: The bidder should undertake to commission the link / services / Router as per SoW within SIX WEEKS from the date of purchase order / letter of Intent
21	Clause 10.3.1	33	The bidder should undertake to commission the link / services / Router as per SoW within FOUR WEEKS from the date of purchase order / letter of Intent	Pls consider 8 weeks	**Change:** The Clause stands modified as under: The bidder should undertake to commission the link / services / Router as per SoW within SIX WEEKS from the date of purchase order / letter of Intent
22	Clause 10.6.1	35	The Bidder should deliver and commission the links including Router within FOUR WEEKS FROM THE DATE OF PURCHASE ORDER / LOI	Pls consider 8 weeks	**Change:** The Clause stands modified as under: The Bidder should deliver and commission the links including Router within SIX WEEKS FROM THE DATE OF PURCHASE ORDER / LOI.
23	Clause 5.2.1	12	Block of /26 IPv4 and block of 256 numbers of IPv6 IPs for each link at DC and DR	Consideration of /29 block of IPv4 for DC and DR locations	No Change
24	5.1.2	12	The last mile and infrastructure including router proposed by the bidder at DC and DR should be scalable to support 256 Mbps during the period of contract.	Vendor the Router bandwidth scalability from 256 as this will impact the commercial. Vendor request SIDBI what will be the timeline of this scalability over period of 6months?	No Change
25	5.4.1	13	The bidder shall provide DDoS attack detection and protection (scrubbing) facility (ONNET) of 1G catering to both DC and DR links (Pool) to filter the traffic as per Bank's requirement.	We request SIDBI to confirm is bidder need to provide DDoS is required in pool (1G in total) or bidder need to provide separate 1G for DC and DR respectively	**Clarification -** DDoS required is pooled among DC and DR.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
26	5.4.2	14	The solution must be able to detect and mitigate different types of Distributed Denial of Service (DDoS) attacks: • TCP SYN Flood • Spoofed TCP-SYN Flood • SYN/ACK Reflection Flood • TCP ACK Flood • Smurf attack • Ping Flood • Ping of Death • ICMP Echo request Flood • Mydoom • UDP Flood • Nuke • HTTP/HTTTPS Flood attack • HTTP/HTTPS Flood attack • DNS amplification attack • IP Fragmented attack • Any other types of flooding attacks	HTTP/HTTPS Flood attack protection requires traffic decryption for which SSL Certificate and private keys of the application is required for mitigating this traffic. Request the Bank to clarify if SSL certifcate and keys will be shared to the service provider else the HTTP/HTTPS flood attack can be mitiagted by implementing an On-Premise DDoS Solution only	Please refer to clause 5.4.2 of the RfP
27	5.4.3	14	The solution must be able to protect all internet protocols used including HTTP, HTTPS, DNS, FTP, IPSEC etc.	HTTPS DDoS Mitigation requires decryption for which SSL Certificates & Private keys are needed. Request SIDBI team to confirm if they are expecting On-premise DDoS device for mitigating HTTPS based DDoS attacks	Please refer to clause 5.4.3 of the RfP
28	Clause 5.4.15.2	14	Detection and Mitigation Process: For Attack more than 1G	Pls clarify on upper limit of DDoS mitigation to be fixed	As per RfP.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
29	5.4.2	14	The solution must be able to detect and mitigate different types of Distributed Denial of Service (DDoS) attacks: • TCP SYN Flood • Spoofed TCP-SYN Flood • SYN/ACK Reflection Flood • TCP ACK Flood • Smurf attack • Ping Flood • Ping of Death • ICMP Echo request Flood • Mydoom • UDP Flood • Nuke • HTTP/HTTTPS Flood attack • HTTP/HTTPS Flood attack • DNS amplification attack • IP Fragmented attack • Any other types of flooding attacks	HTTP/HTTPS Flood attack protection requires traffic decryption for which SSL Certificate and private keys of the application is required for mitigating this traffic. Request the Bank to clarify if SSL certificate and keys will be shared to the service provider else the HTTP/HTTPS flood attack can be mitigated by implementing an On-Premise DDoS Solution only	Please refer to clause 5.4.2 of the RfP
30	5.4.3	14	The solution must be able to protect all internet protocols used including HTTP, HTTPS, DNS, FTP, IPSEC etc.	HTTPS DDoS Mitigation requires decryption for which SSL Certificates & Private keys are needed. Request SIDBI team to confirm if they are expecting On-premise DDoS device for mitigating HTTPS based DDoS attacks	Please refer to clause 5.4.3 of the RfP
31	5.4.8	14	Vendor's solution should have ability to block IPs from any location (known, unknown, suspected geographical locations).	Vendor request SIDBI to amend this clause as the Geographical location based blocking IP is not possible.	No Change
32	5.4.15 1. b) & 2. b)	14	Automatic Attack Mitigation, Mitigation/Scrubbing begins within 30 minutes of attack identification.	Vendor request SIDBI go amend this clause as the auto mitigation is not possible.	**Clarification:** SIDBI to be intimated about the attack and mitigation to be started.
33	5.5.3	15	The bidder should provide interface to SIDBI for monitoring: utilization, performance reports on Real Time, Hourly, Daily, Weekly, Monthly basis.	Vendor wants to notify SIDBI the interface will be only 'read-only'. In case of SIDBI NMS tool integration, vendor request SIDBI to share the NMS platform and its version details with vendor check the possibility of the integration.	**Clarification -** SIDBI requires read only access and NNM integration. Any changes required would be intimated to the service provider and SP is required to do the same.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
34	Clause 5.11.2	16	All the equipment supplied by the bidder [Service Provider] to provide Internet bandwidth should comply with the policies laid down by the Government of India, Department of Telecommunications and should not have any spyware or malware built into it and capable of tracking voice/video and data traffic from a location outside the country	Pls clarify	**Clarification -** The equipment supplied by the bidder should comply all the policies and guidelines issued by GoI, DoT from time to time.
35	Clause 7.6	21	Tender Form Cost: Non-refundable Bid Price of Rs.1,180/-	Consideration for waiver of submission of EMD, being CPSU	No Change
36	Clause 7.7.1	21	EMD: All the responses must be accompanied by a refundable INTEREST FREE security deposit of amount of Rs.1,50,000/-	Consideration for waiver of submission of EMD, being CPSU	No Change
37	9.1.2	30	5 Latency Local Lead <30ms	Bidder assume the latency will be calculated between customer end to provide end router	As per RfP.
38	Service level agreement, Point 7	31	10ms (maximum)	Jitter is a parameter assured in MPLS Links. Leased line Internet, Do not include reporting/measurement/commitment for Jitter value. Request department to remove this clause.	No Change
39	10.3.1	33	2. In the event of non-commissioning of connectivity / delivery of Router, bank will impose LD at the rate of 1% of the order value for late delivered services for every week's delay subject to maximum of 10% of the order value for late delivered services.	Bidder request to amend this clause as: " 2. In the event of non-commissioning of connectivity / delivery of Router, bank will impose LD at the rate of 0.5% of the order value for late delivered services for every week's delay subject to maximum of 5% of the order value for late delivered services."	No Change
40	Clause 11.9.1	39	Performance security: The successful bidder(s) shall provide Performance Security in the form of an unconditional Bank Guarantee (BG) from a scheduled commercial Bank for an amount equivalent to 10% of contract value and valid for period of contract + THREE months (invocation period) from the date of acceptance of the services	Pls consider Performance security of 3%, instead of 10%	No Change
41	Clause 12.4	55-56	Annexure –IV: Commercial Bid	L1 will be based on mandatory services items only or both mandatory and optional services. Pls confirm	**Clarification -** L1 will be based on both the mandatory service items and optional service items (TCO).<<include clarification on table>>

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
42	General	NA	Suggestion	Request the department to include the below compliance standards as part of the DDoS solution from the service providers PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ISO/IEC 27001:2013 (Information Security Management Systems) ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain)	No Change
43	General	NA	Can Single Service provider propose Dual Lastmile, Dual CPE and Dual PE solution for DC & DR. The Secondary lastmile shall be provided from Thirdparty service provider for Redundancy.	This will increase operational efficiency. Request department to amend the same.	No Change
44	General	NA	SLA Exemption	NO SLA penalty will be applicable on bidder incase the location is down due to 1) Power issue at customer end. 2) Improper earthing at site. 3) Equipment damaged due to water seepage or stolen from the location. 4) Access not available at site for the bidder engineer to check the issue. 5) LC not available at site. 6) Any condition which is beyond the control of bidder.	As per RfP.
45	General	NA	Site access and permission	All kind of permission/access at site from feasibility check to link delivery will be arranged by customer. Inbuilding internal cable routing in false celling and under POP wall will be in customer scope of work	As per RfP.
46	General	NA	Power and earthing	RACK Space, Proper power supply and earthing arrangement for the bidder network devices will be arranged and maintained by customer.	As per RfP.

Sr. No.	Clause No.	Page No.	Clause	Query	SIDBI Response
47	General	NA	Network equipment safety	All the network equipments delivered by bidder at customer site for the Services should be kept under safe custody by the customer. In case any device found lost or damaged due to customer attribute than customer has to bear the cost for lost/damaged as well as new device.	As per RfP.
48	General	NA	Site readiness	Customer has to ensure the site readiness before bidder depute engineer at site for installation. Delay due to site readiness will not be consider under the delivery time lines and no penalty or LD will be applicable on bidder.	As per RfP.
49	General	NA	First level troubleshooting	In case of connectivity down, FLT will be done by the customer spoke available at site. No downtime will be attribute to bidder incase the local person is not available at site or on site access is not available for the bidder engineer to check after the FLT.	As per RfP.
50	General	NA	Suggestion	Request the department to include the below compliance standards as part of the DDoS solution from the service providers PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ISO/IEC 27001:2013 (Information Security Management Systems) ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain)	No Change
51			Last date for bid submission		**Change:** **Last date for submission of bids may be read as March 23, 2021; 1530 hrs** **Date & Time of Opening of Minimum Eligibility bid & Technical bid may be read as March 24, 2021; 1130 hrs**

Note: All other terms and conditions are as per RfP and subsequent corrigendums, if any, issued by the Bank against the tender.