Consolidated Queries Received from Prospective Bidders on RFP for Selection of System Integrator for Supply, configuration, implementation, integrations and Maintenance of Distributed Denial of Service (DDOS) Appliances for High Bandwidth Internet Links					
Last Date of Bid Submission is Extended up to 02.06.2022					
Sl. No.	**Clause no.**	**Page no.**	**Clause**	**Query**	**Bank Response**
1		5	Schedule of events and bid details	Request Bank to consider extension of bid submission date	Last date of bid submission is extended up to 02.06.2022.
2	7.6	11	Bank should consider OEM eligibility criteria as well; apart from bidder eligibility criteria.	Proposed OEM's on-premises Anti DDoS solution should have been procured by 3 (PSU /Private) Banks during last 5 years each of minimum 10 Gbps. An email confirmation from bank employee or PO have to be submitted with RFP response.	**Clause no. 7.6 should be read as:** "Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a BFSI/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 5 years. (Supporting document - Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter and/or Certificate of completion of the work). Proposed Appliance (make) should be deployed in atleast three BFSI/RBI/NPCI."
3	7. 2Eligibility Criteria	11	The bidder should be a company registered in India as per Company Act 1956 /2013 or a partnership firm / a Limited Liability Partnership company under the Limited Liability Partnership Act 2008 in India and should be in existence for last 5 years from the date of issuance of RFP. (Certificate of incorporation/certificate for commencement of business/other relevant documentary proof is to be submitted).	We Request bank to exempt this clause for Start-Up India Company with valid Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), (erstwhile Department of Industrial Policy and Promotion), Ministry of Commerce & Industry, Govt. of India DPIIT has issued notification dated 8 November 2016 for Prior turnover and Prior Experience exemption for the start-up recognized organisations registered.	Please be guided by RFP.
4	Eligibility 7.8	12	The Bidder should have at least 5 IT Security professionals who are direct employees of the Bidder having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech) or more on their payroll with certification in CISA or CISSP or CISM. Bidder should have minimum 4 engineers having OEM certification on proposed solution.	Kindly modify the clause and request you to accept the documents post evaluation phase and upon deciding of the successful bidder	**Please read clause as** "The Bidder should have at least 5 IT Security professionals who are direct employees of the Bidder having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech) or more on their payroll, Out of which 1 should be with certification in CISA or CISSP or CISM. Bidder should have minimum 4 engineers having OEM certification on proposed solution."

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
5	7	12	7.5 Eligibility Criteria	Requesting to modify the clause to 'The bidder should be providing IT security services / business (i.e. in the area of implementation, monitoring and management of anti-DDOS solution during last five years. Proof of purchase order/work order/sign off documents showing implementation of various security solutions stated above to be submitted indicating the company is providing such service for the past **2 to 5 years**'	Please be guided by RFP.
6	7.6	12	Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a PSU/ RBI/NPCI (excluding RRB and Co operative Bank) during last 3 years. (Supporting document - Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter and/or Certificate of completion of the work.	We request you to edit this clause as "Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a PSU/ RBI/NPCI/Private BFSI organization (excluding RRB and Co operative Bank) during last 3 years. (Supporting document - Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter and/or Certificate of completion of the work.	**Read clause as,** " "Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a BFSI/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 5 years. (Supporting document - Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter and/or Certificate of completion of the work). Proposed Appliance (make) should be deployed in atleast three BFSI/RBI/NPCI."
7	7.4	12	Bidder should have positive operating Profit (as EBITDA i.e., Earnings efore Interest, Tax, Depreciation & Amortization) in the last three financial years i.e., 2018-19, 2019-20 and 2020-21 as per the audited balance sheet available at the time of submission of tender. In case the audited financials for the year 2020-21 is not finalized, Provisional Balance Sheet of 2020-21 should be submitted. (Copies of the audited balance sheet and Profit/Loss statement of the company are to be submitted.)	We request you to edit this clause as "Bidder should have positive operating Profit (as EBITDA i.e., Earnings efore Interest, Tax, Depreciation & Amortization) in at least 2 of the last three financial years i.e., 2018-19, 2019-20 and 2020-21 as per the audited balance sheet available at the time of submission of tender. In case the audited financials for the year 2020-21 is not finalized, Provisional Balance Sheet of 2020-21 should be submitted. (Copies of the audited balance sheet and Profit/Loss statement of the company are to be submitted.)"	Please be guided by RFP.
8	7.4	12	Bidder should have positive operating Profit (as EBITDA i.e., Earnings Before Interest, Tax, Depreciation & Amortization) in the last three financial years i.e., 2018-19, 2019-20 and 2020-21 as per the audited balance sheet available at the time of submission of tender. In case the audited financials for the year 2020-21 is not finalized, Provisional Balance Sheet of 2020-21 should be submitted. (Copies of the audited balance sheet and Profit/Loss statement of the company are to be submitted.)	We Request bank to Consider Finacial Year's i.e 2019-20, 2020-21, 2021-22 (provisional)	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
9	7.5	12	The bidder should be providing IT security services / business (i.e. in the area of implementation, monitoring and management of anti-DDOS solution during last five years. Proof of purchase order/work order/sign off documents showing implementation of various security solutions stated above to be submitted indicating the company is providing such service for the past 5 years.	We Request bank to exempt this clause for Start-Up India Company with valid Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), (erstwhile Department of Industrial Policy and Promotion), Ministry of Commerce & Industry, Govt. of India DPIIT has issued notification dated 8 November 2016 for Prior turnover and Prior Experience exemption for the start-up recognized organisations registered.	Please be guided by RFP.
10	8.2	13	Overall scope to assist service integrator full coverage of 24*7*365 monitoring & management aspects of anti-DDOS services	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered during the contract period for the proposed solution. Please confirm	Please be guided by RFP.
11	8.1	13	Design, validate, implement & periodically review (preferably OEM review) anti-DDOS solution (along with all the required solution as per scope of work).	As there is no ask for manage service. Design, validate, implement & review should be only limited to the poject deployment	Please be guided by RFP.
12	8.2	13	Overall scope to assist service integrator full coverage of 24*7*365 monitoring & management aspects of anti-DDOS services.	Kindly elaborate. As there is no ask for manage service, what type of assistance is required.	Please be guided by RFP.
13	8.3	13	Assist service integrator as and when required to Identify information security threats/ vectors targeting Bank‘s environment and prevent impact or breach by implementing adequate controls on DDOS appliance to address all kind of DDOS attack.	This scope should be limited only till the project deployment, until project acceptance.	Please be guided by RFP.
14	9. Detailed Scope	14	Bidder shall propose solution that should be capable of retrieving the archived logs for analysis, correlation, reporting and forensic purposes. Appliance shall be capable of retaining the logs locally for minimum period of 3 months.	What is the estimated log size to be considered for 3 month log retention	Bidder need to derive the log size based on the proposed box size with maxuimum throuhput utilisation.
15	8.4	14	Ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the identified locations by Bank), enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, backups, audits, support for the proposed hardware/software required for delivering the managed Security Support services.	If there is a relocation during the deployment phase, our understanding is the lift and shift would be done by the Bank.. The understanding is the mentioned points in the clause will be freezed before the deployment starts during the kick-off meeting. Post deployment sign-off, this will not be a part of scope of management and operations of Bidder as Bidder is not providing the same. Please confirm	Transportation/shifting , if any will be taken care by the Bank. All remaining activities shall be taken care by the bidder

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
16	8.5	14	The service delivery (SLA Management) and periodic review reporting.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Hence the clause will not be applicable to the bidder. Please confirm	**Clause no. 8.5 should be read as:** "The service delivery (SLA Management in terms of appliance related issues) and periodic review reporting."
17	9.7	14	SOP should also cover log monitoring tool management including configuration, agent deployments, backup, and recovery.	Our understanding is Bidder is not providing any log monitoring tool. Hence request you to temove this clause	Log monitoring tool integration here refers to integration of appliance with SIEM tool.
18	9.8	14	Bidder should provide knowledge transfer and training on the technology, functionality and operations of the anti-DDOS solution to current service integrator and Bank officials.	Please confirm on the no of participants for the training and the location for the training to be conducted	knowledge transfer and training on the technology, functionality and operations of the propsoed anti-DDOS solution to 15 participants
19	9.12	14	In case of any incident, bidder should identify the root cause of the attack & suggest preventive measures to avoid facing similar type of attacks again.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered during the contract period for the proposed solution. Please confirm	**Caluse no. 9.12 should be read as:** "In case of any incident, bidder should support current service provider if required to identify the root cause of the attack & suggest preventive measures to avoid facing similar type of attacks again."
20	9.1	14	Solution should be capable of integration with SIEM, PIM, MFA etc. and vendor must integrate it with Bank’s CSOC solutions.	Kindly share the details of the SIEM, PIM, MFA solution (vendor name & Model)	Details shall be shared with successful bidder
21	8.5	14	The service delivery (SLA Management) and periodic review reporting.	This scope should be with your current SI who will manage the DDoS CPE	**Clause no. 8.5 should be read as:** "The service delivery (SLA Management in terms of appliance related issues) and periodic review reporting."
22	9.5	14	Provide assistance to Bank’s SI if needed during cyber security drills / audits as and when conducted.	This scope should be with your current SI who will manage the DDoS CPE	Provide assistance to Bank’s SI, if needed, during cyber security drills / audits.
23	9.6	14	Assist service integrator providers if required, in Alerting events / incidents and recommending remedial actions.	This scope should be limited only till the project deployment, until project acceptance.	Please be guided by RFP.
24	11	15	The bidder is expected to supply, installation & maintenance of comprehensive Anti-DDoS solution on-premise appliance.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Please confirm	Please be guided by RFP.
25	12 e	16	Bidder is responsible for developing and implementing the security configuration hardening of proposed anti-DDOS solution. Also, they have to periodically review the guidelines and configure as and when required.	Our understanding is this will be provided during the implementation phase. Post implementation, the existing Bank/partner will manage the same. Please confirm	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
26	13.2 Implementation Instructions and Extended Scope	17	The Bidder, in coordination with OEM do a gap analysis and submit a detailed study of the Bank‘s infrastructure and requirements relating to the anti-DDOS solution, prepare a detailed plan document/ road map mentioning all the pre- requisites, time-frame of mile-stones/ achievements leading to the full operationalization of the solution vis-à-vis Bank‘s requirement. This exercise should not affect the normal day to day functionality of the Bank.	Please provide detailed scope of the clause	Please be guided by RFP.
27	13.7	17	Implementation of solution must follow various standards such as ISO 27001:2013, PCI DSS, ISO 22301 etc. Bidder should assist service integrator to close observations in various audits of the proposed solution in co-ordination with current CSOC FM service provider at Bank.	Our understanding is the observations of the various audits mentioned in the clause will be shared during the implementation phase. Since management and monitoring will be done by Bank's existing team/partner, observations of the audits during this phase will be managed by the Bank's existing team/partner. Please confirm	Please be guided by RFP.
28	13.18	18	DDOS Solution hardware shall be capable of inspection as well as mitigation throughput of 30 Gbps. Bank will procure licenses for 10 Gbps inspection as well as mitigation throughput at day one. Bank may upgrade the throughput in future at discovered price of 10 Gbps throughput.	Our understanding is hardware needs to be sized for 30Gbps from day one and scrubbing license for 10Gbps from day one. Please confirm	Please be guided by RFP.
29	13.18	18	DDOS Solution hardware shall be capable of inspection as well as mitigation throughput of 30 Gbps. Bank will procure licenses for 10 Gbps inspection as well as mitigation throughput at day one. Bank may upgrade the throughput in future at discovered price of 10 Gbps throughput.	Kindly confirm if the bidder needs to procure the scrubbing from the OEM or the Bank's Internet service provider	Scrubbing from ISP shall be taken care by the Bank.
30	13.18	18	DDOS Solution hardware shall be capable of inspection as well as mitigation throughput of 30 Gbps. Bank will procure licenses for 10 Gbps inspection as well as mitigation throughput at day one. Bank may upgrade the throughput in future at discovered price of 10 Gbps throughput.	If it is Banks ISP, request Bank to keep the procurement of the scrubbing license out of the RFP	Scrubbing from ISP shall be taken care by the Bank.
31	13.19	18	The Bidder must also carry out preventive maintenance of the setup implemented on both DC & DR which includes periodic upgrade & enhancements.	Since additional PS effort will be required. By the term periodic, should the bidder consider this activity as once a year?	Upgrades & enhancements should be in sync with upgrades patches released by OEM.
32	13.27	19	Adherence to agreed Service Level Agreements (SLA) and periodic review of solution should be conducted by bidder for continual improvement of the solution.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered during the contract period for the proposed solution. Hence the SLA willnot be applicable to the bidder. Request you to consider the same	SLA would be calculated after the ticket is raised with the bidder.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
33	13.30	19	Anti-DDOS setup maybe subjected to audit from Bank and/or third party and/or regulatory body. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors with co-ordination with onsite team. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty as defined in SLA.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered/audit points to be closed during the contract period for the proposed solution. Hence the SLA willnot be applicable to the bidder. Request you to consider the same	Please be guided by RFP.
34	14.1 Project Implement ation Plan	20	Appliances and software licenses must be delivered within 9 weeks from the issue of purchase order to the successful Bidder.	Request you to modify the hardware delivery timelines to 10-12 weeks	**Caluse no. 14.1 should be read as:** "Appliances and software licenses must be delivered within 10 weeks from the issue of purchase order to the successful Bidder."
35	14.2 Project Implement ation Plan	20	The Bidder shall complete the configuration, implementation, integrations within 3 weeks from date of delivery. Any delay beyond stipulated period will attract additional penalty, as mentioned in the LD clause. Part of the week will be considered as full week.	Request you to modify the implementation timelines to 5-6 weeks	**Caluse no. 14.2 should be read as:** "The Bidder shall complete the configuration, implementation, integrations within 5 weeks from date of delivery. Any delay beyond stipulated period will attract additional penalty, as mentioned in the LD clause. Part of the week will be considered as full week."
36	13.31	20	Bench Marking: The bidder will demonstrate the benchmarking tests to confirm compliance with the stated functionalities.	Please clarify what are the parameters for benchmarking tests	Benchmarking would require the demonstration of Anti DDOS capabilities as per RFP specifications.
37	13.33	20	SLA Compliance: The bidder shall ensure compliance with SLAs as defined in the RFP.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered to be closed during the contract period for the proposed solution. Hence the SLA willnot be applicable to the bidder. Request you to consider the same	Please be guided by RFP.
38	13.33	20	SLA Compliance: The bidder shall ensure compliance with SLAs as defined in the RFP.	Asked in the RFP is for 1 unit each in DC and DR and SLA asked is 99.5%. If the device goes down, it will take few hours to replace the product	Please be guided by RFP.
39	14.1	20	Appliances and software licenses must be delivered within 9 weeks from the issue of purchase order to the successful Bidder.	We request you to consider the below timelines - Appliances and software licenses must be delivered within 12 weeks from the issue of purchase order to the successful Bidder.	**Clause no. 14.1 should be read as:** "Appliances and software licenses must be delivered within 10 weeks from the issue of purchase order to the successful Bidder."

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
40	14.2	20	The Bidder shall complete the configuration, implementation, integrations within 3 weeks from date of delivery. Any delay beyond stipulated period will attract additional penalty, as mentioned in the LD clause. Part of the week will be considered as full week.	We request you to consider the below timelines - The Bidder shall complete the configuration, implementation, integrations within 6 weeks from date of delivery. Any delay beyond stipulated period will attract additional penalty, as mentioned in the LD clause. Part of the week will be considered as full week.	**Clause no. 14.2 should be read as:** "The Bidder shall complete the configuration, implementation, integrations within 5 weeks from date of delivery. Any delay beyond stipulated period will attract additional penalty, as mentioned in the LD clause. Part of the week will be considered as full week."
41	14.1	20	Appliances and software licenses must be delivered within 9 weeks from the issue of purchase order to the successful Bidder	This is a very small time period, we request you to change the clause as "Appliance an software licenses must be delivered within 12 weeks from the issue of purchase order of successful bidder	**Clause no. 14.1 should be read as:** "Appliances and software licenses must be delivered within 10 weeks from the issue of purchase order to the successful Bidder."
42	Phase VI-Monitoring, Management & Sustenance	22	Post-deployment (after sign-off) bidder will manage & monitor DDOS solution.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Please confirm	**Clause no. Phase VI - Monitoring, Mnagement & Sustenance should be read as:** "Post-deployment (after sign-off) bidder will assisst current SI to manage & monitor DDOS solution."
43	27. Payment Terms	39	Point No: 4: On Project sign off and against Performance Bank Guarantee (PBG) - 10%	Out of 100 % payment last 10 % payment is against Project sign off and PBG, request you to kindly make the final 10% payment against submission of PBG by the bidder.	Please be guided by RFP.
44	27. Payment Terms	39	Point No: 4: On Project sign off and against Performance Bank Guarantee (PBG) - 10%	Request SEBI team to kindly explain in detail what are the expectations for the Sign off criteria as 10 % payment is against the same line item	Signoff shall be provided based on the successful implementation of DDOS solution as per RFP requirements.
45	26	39	In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc. arising from the use of the procurement of this RFP or any part/ component thereof in India, the Supplier shall act expeditiously to extinguish such claim. If the Supplier fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Supplier shall be responsible for the compensation including all expenses, court costs and lawyer fees. The Bank will give notice to the Supplier of such claim, if it is made, without delay.	We request to include the remedy for IP Infringment as:- In the event of a third party claim of intellectual property infringement, Bidder may, at its sole option, (i) obtain for Customer the right to continue using the Services, (ii) modify the Services so that the Services are non-infringing, (iii) replace the Services with a functionally equivalent, non-infringing service, or (iv) if the alternatives in Section (i)-(iii) are not available, Bidder may so notify Bank and terminate such infringing Services without penalty to either Party. We request you to add the following exceptions to the said clause: 1. Not using the said products in combination with other products not provided by the bidder or 2. equipments not being used as per the instructions provided by the bidder.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
46	28 - Order Cancellation	40	22 Order Cancellation 22.14 The Bank reserves its right to cancel the Purchase Order at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions: 22.1.1. Delay in commencement of the project beyond two weeks after the assignment order or beyond the date given by the bank in the purchase order. 22.1.2. Delay in completion of project. 22.1.3. Serious discrepancies noted in the inspection. 22.1.4. Breaches in the terms and conditions of the Order. 22.15 The Bank reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by the Bank on the following circumstances: 22.2.1. Non-submission of acceptance of order within 7 days of order. 22.2.2. Excessive delay in execution of order placed by the Bank. 22.2.3. The selected bidder commits a breach of any of the terms and conditions of the bid. 22.2.4. The bidder goes in to liquidation voluntarily or otherwise. 22.2.5. The progress made by the selected bidder is found to be unsatisfactory. 22.2.6. Bidder provides evasive or incorrect information. 22.16 After the award of the contract, if the selected bidder does not perform satisfactorily or delays	NTT Comment: Please confirm that in case of any termination for default Bidder shall be provided with 30 days written notice to cure or remedy such default and the contract shall not be terminated if the default is cured within the cure period. For all practical purposes, please confirm that termination of the agreement shall not affect the payment rights of the Bidder for work successfully rendered till the date of termination and Bank will only have the right to recover or deduct applicable LD/penalties agreed under the Agreement. Please confirm that there is no termination for convenience.	Please be guided by RFP.
47	27.4	40	Payment terms	Payment term Slab asked by UBI . 50% /30%/10%/10% . Request UBI to amend Slab to 80%/10%/5%/5%	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
48	The terms of payment	40	The terms of payment will be as follows: 1 On delivery of Hardware with System Software at Both DC and DR sites. 50% 2 On completion of installation, configuration, integrations and commissioning of DDOS appliances at Both DC and DR sites. 30% 3 On activation of 10 Gbps scrubbing licences with 3 years warranty 10% 4 On Project sign off and against Performance Bank Guarantee (PBG) 10%	Request you to change as "The terms of payment will be as follows: 1 On delivery of Hardware with System Software at Both DC and DR sites. 70% 2 On completion of installation, configuration, integrations and commissioning of DDOS appliances at Both DC and DR sites. 10% 3 On activation of 10 Gbps scrubbing licences with 3 years warranty 10% 4 On Project sign off and against Performance Bank Guarantee (PBG) 10%"	Please be guided by RFP.
49	30.1	42	Bidder is expected to provide unconditional warranty for DDOS Hardware and 10 Gbps scrubbing licenses for 3 years and post-warranty (AMC/ATS) for 2 years comprehensive on-site 24x7 maintenance support for problem resolution commitment for 5 years.	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Please confirm	Please be guided by RFP.
50	32	43	OEM Authorization	Bank to share the MAF format	Suggested format with required confirmation from OEM is provided under RFP Clause 7.7
51	33. Liquidatied Damages	44	LD for delay in delivery/ installation/implementation/ deployment of licenses for each week of delay beyond the scheduled commencing date or part thereof will be a sum equivalent to 0.5% of order value or unperformed Services. In case of undue delay beyond a period of 15 days after attaining the maximum penalty of 5% of total project cost excluding AMC/ATS cost, Bank may consider termination of the contract or purchase order. 33.2 The overall LD during implementation will be to a maximum of 5% of the total cost of the project excluding AMC/ATS cost.	This clause is confusing hence request you to kindly clarify, what is the maximum penalty for delay in delivery and what is the maximum penalty for implementation delay. Is it on the undelivered / unperformed products or on total project cost.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
52	33	44	**Liquidated Damages (LD)** If Successful **bidder fails to deliver** any or all of the Service(s) / Systems **or perform the Services within the time period(s)** specified in the RFP/Contract / Agreement, BANK shall, without prejudice to its other rights and remedies under and in accordance with the RFP/Contract / Agreement, levy Liquidated Damages (LD) from payments, which are due to the Successful bidder. For calculation of LD: 33.1 LD for delay in delivery/ installation/implementation/ deployment of licenses for each week of delay beyond the scheduled commencing date or part thereof will be a **sum equivalent to 0.5% of order value or unperformed Services**. In case of **undue delay beyond a period of 15 days after attaining the maximum penalty of 5% of total project cost excluding AMC/ATS cost**, Bank may consider termination of the contract or purchase order. 33.2 The **overall LD** during implementation will be to a **maximum of 5% of the total cost of the project** excluding AMC/ATS cost. 33.3 Part of week will be considered as full week. 33.4 Any delay by the bidder in performance of its delivery obligations shall render the bidder liable to the imposition of liquidation damages, unless extension of time is agreed upon without application of liquidation damages. 33.5 Bank can deduct the amount of liquidated damages from any money belonging to the Successful bidder in its hands (which includes BANK's right to claim	Commercial Team to confirm. Suggestion: The delay and non-performance should be solely attributable to the Bidder. Also, the delay should recovered through Service credits and damages must be capped @ 12 months charges paid to Tata Comm.	Please be guided by RFP.
53	34.4	45	Supplier shall ensure that a minimum 99.5% uptime of the solution is maintained monthly (Calculated on a quarterly basis, which includes all of the solutions as a whole).	Request you to revise the Uptime SLA to 99.5% Kindly confirm if this is device level SLA or solution level (HA model) at each site.	Please be guided by RFP.
54	34.4	45	Supplier shall ensure that a minimum 99.5% uptime of the solution is maintained monthly (Calculated on a quarterly basis, which includes all of the solutions as a whole).	Our understanding is Bidder only needs to supply and implement. Management and Monitoring will be done by the existing Bank's team/partner. Bidder can provide support as and when Bank raises a ticket to provide assistance for issues encountered to be closed during the contract period for the proposed solution. Hence the SLA will not be applicable to the bidder. Request you to consider the same	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
55	34.4	45	Uptime is greater than or equal to 99.50%	As there is no ask for manage service. Uptime should be UBI's SI responsibility. In hardware solution deployement the should only RMA replacement timeline. Uptime is applicable if it is a platform, although here we are talking about an appliance which is in customer DC, hence uptime ca not be deployed by the provider	Please be guided by RFP.
56	34.4	45	SLA penalty	Penalty Slab asked by UBI . 2%/5%/Penalty at an incremental rate of 1% of cost of quarterly recurring payment for every 0.1% lower than the stipulated uptime. Request UBI to amend Slab to 1%/2%/Max capiing upto 5% of quarterly payment .	Please be guided by RFP.
57	34.12	46	The penalty, including LD is capped at maximum 10 % of TCO.	Kindly revise the LD at maximum 5% of TCO	Please be guided by RFP.
58	34.11	46	RBI/Regulatory authority may inspect facilities of successful bidder up to 2 years beyond the contract period.	Our understanding is Bidder is not providing any platform services. Proposed solution is going to be deployed in Bank's premises. Hence need clarity about the inspection of the Bidder's facility	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
59	36	46	**Confidentiality** The bidder must undertake that they shall hold in trust any Information received by them, under the Contract/Agreement, and the strictest of confidence shall be maintained in respect of such Information. The bidder has also to agree: 36.1 To maintain and use the Information only for the purposes of the Contract/Agreement and only as permitted by the BANK; 36.2 To only make copies as specifically authorized by the prior written consent of the Bank and with the same confidential or proprietary notices as may be printed or displayed on the original; 36.3 To restrict access and disclosure of Information to such of their employees, agents, strictly on a “need to know” basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause and 36.4 To treat all Information as Confidential Information. 36.5 The Selected Bidder shall be required to sign a Non-Disclosure Agreement with Bank as per prescribed format provided in Annexure J within thirty days of issuing the purchase order/letter of intent.	Request you to make the clause mutual to protect bidder's confidential information	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
60	37	46	**Indemnity & Limitation of Liability** 37.1.Subject to Clause 37.4 below, the bidder (the "Indemnifying Party")undertakes to indemnify, hold harmless the Purchaser (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively “Loss”) on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or willful default in performance or non-performance under this Agreement. 37.2.If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party. 37.3.Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by: 37.3.1.Indemnified Party’s misuse or modification of the Service; 37.3.2.Indemnified Party’s failure to use corrections or enhancements made available by the Indemnifying Party; 37.3.3.Indemnified Party’s use of the Service in	Suggestion:Indemnity obligation to be limited to third party claims. Incase of IP infringment the exclusive remedy should be (i) obtain for Customer the right to continue using the Services, (ii) modify the Services so that the Services are non-infringing, (iii) replace the Services with a functionally equivalent, non-infringing service, or (iv) if the alternatives in Section (i)-(iii) are not available, Bidder may so notify Bank and terminate such infringing Services without penalty to either Party. Indemnity of Tata Comm to be capped @ 12 months charges paid to Tata Comm	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
61	38	49	**Intellectual Property Rights** The Bidder claims and represents that it has obtained appropriate rights to provide/use the Deliverables and Services upon the terms and conditions contained in this RFP. 38.1 The Bidder shall be responsible at its own cost for obtaining all necessary authorizations and consents from third party licensors of Software used by Bidder in performing its obligations under this Project. 38.2 If a third party's claim endangers or disrupts the Bank's use of the Deliverables, the Bidder shall at no further expense, charge, fee or cost to the Bank, (i) obtain a license so that the Bank may continue use of the Deliverables in accordance with the terms of this RFP. 38.3 Bidder shall indemnify and keep fully and effectively indemnified the Bank from all legal actions, claims, or damages from third parties arising out of use of software, designs or processes used by Bidder or his subcontractors or in respect of any other services rendered under this RFP.	Suggested: To add that Bank is and shall remain exclusively entitled to all right and interest in and to all Bank Technology, and Bidder is and shall remain exclusively entitled to all right and interest in and to all Bidder Technology. Bank shall not, directly or indirectly, reverse engineer, de-compile, disassemble or otherwise attempt to derive source code or other trade secrets from Bidder Technology. We request to include the remedy for IP Infringment as:- In the event of a third party claim of intellectual property infringement, Bidder may, at its sole option, (i) obtain for Customer the right to continue using the Services, (ii) modify the Services so that the Services are non-infringing, (iii) replace the Services with a functionally equivalent, non-infringing service, or (iv) if the alternatives in Section (i)-(iii) are not available, Bidder may so notify Bank and terminate such infringing Services without penalty to either Party.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
62	42 - Exit Clause	50	37 Exit Clause The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions: 37.1 Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 30 days from receipt of purchase contract. 37.2 Delay in delivery beyond the specified period. 37.3 Delay in completing testing/customization and acceptance tests/ checks beyond the specified periods; 37.4 Serious discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution. In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period. NTT Comment: Please confirm that any exit from the contract due to default on the part of the Bidder, will be done after 30 days written notice to the Bidder is to cure or remedy such default and the contract shall not be terminated if the default is cured within the cure period. Further, please confirm that termination of the agreement shall not affect the accrued rights and liabilities of Parties arising prior to the termination date.	NTT Comment: Please confirm that any exit from the contract due to default on the part of the Bidder, will be done after 30 days written notice to the Bidder is to cure or remedy such default and the contract shall not be terminated if the default is cured within the cure period. Further, please confirm that termination of the agreement shall not affect the accrued rights and liabilities of Parties arising prior to the termination date.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
63	43 Termination of Contract	50	38 Termination of Contract If the Termination is on account of failure of the successful bidder to perform the obligations under this RFP contract, the Bank shall have the right to invoke the Performance Bank Guarantee(s) given by the selected bidder. The Bank will be entitled to terminate this Contract, without any cost to the Bank and recover expenditure incurred by Bank, on the happening of any one or more of the following: 38.1 The selected bidder commits a breach of any of the terms and conditions of the bid. 38.2 The Successful bidder goes into liquidation voluntarily or otherwise 38.3 An attachment is levied or continues to be levied for a period of 7 days upon effects of the Agreement. 38.4 The progress regarding the execution of the order accepted by the selected bidder is found to be unsatisfactory or delay in execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which Bank may have to incur in executing the balance contract. This clause is applicable, if for any reason, the contract is cancelled. 38.5 Non-satisfactory performance of the selected bidder during implementation and operation. 38.6 An act of omission by the Bidder, its employees, its	NTT Comment: Please confirm that in case of any termination for default Bidder shall be provided with 30 days written notice to cure or remedy such default and the contract shall not be terminated if the default is cured within the cure period. For all practical purposes, please confirm that termination of the agreement shall not affect the payment rights of the Bidder for work successfully rendered till the date of termination and Bank will only have the right to recover or deduct applicable LD/penalties agreed under the Agreement.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
64	41	50	**Force Majeure** Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the Contract, such as: 41.1 Natural phenomena, including but not limited to floods, droughts, earthquakes, epidemics, 41.2 Acts of any Government, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes, 41.3 Terrorist attacks, public unrest in work area; Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Bidder or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and/or defined above.	Suggestion to add exception: Except for Bank's payment obligations accruing under this Agreement up to the date of a bona fide Force Majeure Event	Please be guided by RFP.
65	43	50	**Termination of Contract**	We can provide the SLAs in case of discepancies of the Services. Bank and Bidder can mutually discuss to reach upto a solution.	Please be guided by RFP.
66	44 Audit	51	39 Audit The Bidder shall at all times whenever required furnish all information, records, data stored in whatsoever form to internal, external, Bank appointed and statutory/ RBI inspecting auditors and extend full cooperation in carrying out of such inspection. The Bidder will also undertake to co-operate with the RBI to carryout its supervisory functions and objectives and will furnish all records and other information as RBI may call for to carry our inspection and/ or other functions. The Bidder is required to facilitate the same at no additional cost and shall provide uninterrupted access to the documents required by the auditors. Further the Bidder has to ensure rectification of all the irregularities thus pointed out by the auditor within a given time frame.	NTT Comment: Please confirm that the request for audit shall strictly be in linked to the scope of work and not include disclosure of any financial information, like books of accounts, cost break-up, profit margins etc. Further, please confirm that any audit by the Bank or Bank appointed third party shall be done after prior written notification to the Bidder.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
67	53	54	Availability of Spares	Our understanding is Bidder needs to be provide 4 appliances - 2 in DC and 2 in DR out of which 2 (1in DC and 1 in DR) will be spare and will be at Bank's premises and this needs to be provided from day 1 for the entire contract period	**Clause no. 53 should be read as:** "Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off at market and should not become end of life. RMA for the hardware/software offered should be available in bank premises within 8 hours of appliance failure after raising the ticket."
68	53	54	Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off at Bank’s premises.	**Bank to Consider** - Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off in Country.	**Clause no. 53 should be read as:** "Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off at market and should not become end of life. RMA for the hardware/software offered should be available in bank premises within 8 hours of appliance failure after raising the ticket."
69	54	54	**Insurance** The insurance is to be taken by Bidder for an amount equal to 110% of the CIF value of the goods delivered at the respective sites covering all risks (including fire, burglary, SRCC, natural calamities such as earth quake, flood etc.) up to installation and configuration of hardware after the delivery at both the sites.	Suggestion to delete this clasue and add the following: Each Party shall keep in full force and effect during each Service Term insurance cover which is no less than that required by applicable law and is customary in accordance with best industry standards. If requested in writing by the other Party, a Party will provide certificates of insurance evidencing its insurance coverage.	Please be guided by RFP.
70	Pre-Qualification Criteria Point 5	59	The bidder should be providing IT security services / business (i.e. in the area of implementation, monitoring and management of anti-DDOS solution during last five years.	Request you to change as "The bidder should be providing IT security services / business during last five years." to allow more participation	Please be guided by RFP.
71	Pre-Qualification Criteria Point 6	59	Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a PSU/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 3 years..	Request you to change as "Bidder should have implemented anti-DDOS services devices in at least One corporates/Gov/PSU/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 3 years.."to allow more participation	**Clause no. Pre-Qualification Criteria Point 6 should be read as:** "Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a BFSI/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 5 years. Proposed Appliance (make) should be deployed in atleast three BFSI/RBI/NPCI."

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
72	Pre-Qualification Criteria Point 8	60	The Bidder should have at least 5 IT Security professionals who are direct employees of the Bidder having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech) or more on their payroll with certification in CISA or CISSP or CISM. Bidder should have minimum 4 engineers having OEM certification on proposed solution.	Request you to change as "The Bidder should have at least 5 IT Security professionals who are direct employees of the Bidder having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech) or more on their payroll Out of which 1 should be with certification in CISA or CISSP or CISM. Bidder should have minimum 4 engineers having OEM certification on proposed solution."	**Please read clause as** "The Bidder should have at least 5 IT Security professionals who are direct employees of the Bidder having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech) or more on their payroll, Out of which 1 should be with certification in CISA or CISSP or CISM. Bidder should have minimum 4 engineers having OEM certification on proposed solution."
73	10	61	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key	Based on the industry standard for 10G traffic 4000 SSL CPS / TPS is very less.. Request Bank to increase to 40,000 SSL CPS / TPS and scalable upto 90,000 SSL CPS/TPS.	**Please read clause as,**"SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 90000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key"
74	6	61	Solution should support minimum of 32 Million packet per seconds	1.Packets per second (PPS) is one of the most important measurements to consider when planning a DDoS defense strategy and evaluating solutions. Protocol or network-layer DDoS attacks send large numbers of packets to targeted network infrastructures and infrastructure management tools. These protocol attacks include SYN floods and Smurf DDoS, among others, and their size is measured in packets per second (PPS). On a Gigabit link, for example, you can have anywhere from tens of thousands to millions of packets. In DDoS, an attacker's strategy is asynchronous, meaning the attacker attempts to do as little work as possible while making their target do a lot of work. Therefore, attackers tend to use smaller packets and force the target to respond with larger packets in response, which drains the target's resources. Smallest packets commonly seen on networks is a TCP ACK packet. TCP ACK packet has a 20 byte IP header and a 20 byte TCP header, adding up to 40 bytes. Because this is smaller than ethernet's minimum payload size of 46 bytes, it is automatically padded prior to transmission to bring it up to size. It is then wrapped with a 14 byte header and 4 byte CRC, to give the minimum ethernet frame size of 64 bytes When transmitted, each packet must also be preceded by a 7-byte preamble and 1-byte start-of-frame delimiter and must be followed by an inter-frame gap of at least 12 bytes. This makes the smallest transmission in ethernet effectively 84 bytes. Calculate the maximum packet rate of 84 bytes on a 10G link: 10Gbps / (84 bytes * 8 bits) = 14.88Mps	Please be guided by RFP

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
75	Annexure D-10	61	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key	Based on the industry standard for 10G traffic 4000 SSL CPS / TPS is very less.. Request Bank to increase to 40,000 SSL CPS / TPS and scalable upto 90,000 SSL CPS/TPS.	Please be guided by RFP.
76	6	61	Solution should support minimum of 32 Million packet per seconds	Understanding the asked of throughput of 10Gbps scalable to 30Gbps. Smallest packet size that can land on any network as per RFP standards is 84 Bytes Now as per calculation to size Packets per Second i.e. **PPS x Packet Size (bytes) = Bandwidth (Bps)** for **10Gbps of traffic** Packets per Seconds should be ~15,238,095 PPS i.e. **15MPPS** And for **30Gbps** of Traffic Packets Per Seconds should be ~ 45,714,285 PPS i.e. **45MPPS** Which is more than asked i.e. 32 MPPS Now understanding the enterprise network, which can maximum absorb 40% of attack traffic to be mitigated on-premise and any traffic beyond this will be scrubbed by Cloud service *(Incase of UBI with 30Gbps of link comes to 12Gbps - considering 40% attack, as per best practice link utilization should be approx. 60-70% only and spare bandwidth will be 30-40%* **With above understanding the Packets per Second requirement can come to ~20MPPS - 25MPPS** **Hence request to modify the specs to below** Solution should support minimum of 20 Million packet per seconds	Please be guided by RFP
77	10	61	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key	DDoS Solution is meant to block large flood attacks, and there can be no upper limit to be able to mitigate SSL flood attacks **To be able to mitigate the DDoS Flood Attack need to increase the SSL CPS at least 20 times** **Hence request to change the spec to below** SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 80,000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key	Please be guided by RFP

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
78	10	61	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key	DDoS Solution is meant to block large flood attacks, and there can be no upper limit to be able to mitigate SSL flood attacks **To be able to mitigate the DDoS Flood Attack need to increase the SSL CPS at least 20 times and should be scalable in future with either internally or externally** **Hence request to change the spec to below** SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 80,000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key and this SSL CPS should be scalable to as per Banks requirement internally or Externally	Please be guided by RFP
79	47	63	System should have mitigation mechanism to protecting against zero- day DoS and DDoS attacks without manual intervention and response time should be less than 2 seconds.	Zero-day attacks mitigation for any appliances needs signature creation to be tuned as per attack flood to minimize false positive less than 2 seconds is very aggressive number and no OEM can match this expectation of mitigating Zero-Day attack within 2 seconds without developing its signature **Hence request to change the specs to below** System should have mitigation mechanism to protecting against zero- day DoS and DDoS attacks without manual intervention and response time should be less than 1 minutes.	**Please read the clause as**, "System should have mitigation mechanism to protecting against zero- day DoS and DDoS attacks without manual intervention and response time should be less than 20 seconds."
80	60	64	Solution should support Flowspec	DDOS Appliance is deployed inline which works on packet based detection in realtime and mitigates the all types of DDOS attacks. Flowspec is a feature supported from routers to drop certain type of specific traffic based on protocal / source / destination IP. **Request Bank to Consider - Solution should support Flowspec / Real time packet analysis**	Line Item 60 of Annexure D stands deleted.
81	Annexure D-60	64	Solution should support Flowspec	DDOS Appliance is deployed inline which works on packet based detection in realtime and mitigates the all types of DDOS attaks. Flowspec is a feature supported from routers to drop certain type of specific traffic based on protocal / source / destination IP. **Bank to Consider** - Solution should support Flowspec / Real time packet analysis	Line Item 60 of Annexure D stands deleted.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
82	60	64	Solution should support Flowspec	Flowspecs protocol used by ISP to mitigate the attack on their Routers leveraging Orchestrator and additional component This is not relevant to enterprise DDoS Mitigation Solution. Since for Enterprise, DDoS appliance will be first line of defense and no third party component is present **Hence request to delete the specs**	Line Item 60 of Annexure D stands deleted.
83	62	64	System must detect and block HTTP Opcode Flood	Opcode is not relevant to HTTP Protocol. And more relevant to DNS security vulnerability **Hence request to delete the specs**	Line Item 62 of Annexure D stands deleted.
84	67	64	The system should be able to work in fail open mode in all the ports (including copper and fiber) and should support software bypass capability. Solution should have built-in hardware bypass for all interface types and Separate hardware based bypass switch wouldn't be accepted.	Every OEM have different ways to handle bypass capability And most of the OEM have Bypass switch capability via external appliance and only one OEM have in build bypass for only one appliance **Hence request to change the specs to below** The system should be able to work in fail open mode in all the ports (including copper and fiber) and should support software bypass capability. Solution should have hardware bypass for all interface types either internally or Externally	**Please read the clause as**,"The system should be able to work in fail open mode in all the ports (including copper and fiber) and should support software bypass capability. Solution should have hardware bypass for all interface types either internally or Externally"
85	82	65	Should support IP defragmentation, TCP stream reassembly.	IP defragmentation, TCP stream reassembl is a function of Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - Should support IP defragmentation / fragmentation related DDOS attacks.	Please be guided by RFP
86	Annexure D-82	65	Should support IP defragmentation, TCP stream reassembly.	IP defragmentation, TCP stream reassembl is a function of Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - Should support IP defragmentation / fragmentation related DDOS attacks.	Please be guided by RFP

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
87	75	65	The proposed solution should support integration of external Threat Intelligence Platform (TIP)	Integration with Threat Intelligence feed with respect to DDoS appliance doesn't make sense, since DDoS appliance is meant to block DDoS related threats and DDoS appliances has to act as an Stateless appliances. Allowing such feeds to be inspected by URL/Hash/Domains would need DDoS appliance to decrypt all the traffic making it Stateful defying the purpose of DDoS Solution **Hence request you to change this specs to:** The proposed solution should support integration of Threat Intelligence Platform (TIP)	**Please read the clause as,**"The proposed solution should support integration of Threat Intelligence Platform (TIP)"
88	98	66	System should support Intrusion Prevention from Known Attacks either on the appliance or through external appliance	Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - DDOS mitigation system should provide comprehensive outbound traffic blocking for C&C, malware drop points, bad reputation IP/Domain/URL traffic.	Line Item 98 of Annexure D stands deleted.
89	104	66	Proposed solution should Protect against SSL & TLS-encrypted information leaks with a separate SSL Decryption module on device / out of Path	TLS-encrypted information leaks is a function of Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - DDOS mitigation system should provide comprehensive outbound / Inbound traffic blocking for C&C, malware drop points, bad reputation IP/Domain/URL traffic.	Please be guided by RFP
90	97	66	System should support anti-evasion mechanisms	Anti evasion is a function / feature of IPS **Bank to Consider** - System should support anti-evasion or anti-bot mechanisms	Line Item 97 of Annexure D should be read as,"System should support DDOS anti-evasion "
91	Annexure D-98	66	System should support Intrusion Prevention from Known Attacks either on the appliance or through external appliance	Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - DDOS mitigation system should provide comprehensive outbound traffic blocking for C&C, malware drop points, bad reputation IP/Domain/URL traffic.	Please be guided by RFP
92	Annexure D-104	66	Proposed solution should Protect against SSL & TLS-encrypted information leaks with a separate SSL Decryption module on device / out of Path	TLS-encrypted information leaks is a function of Intrusion prevention system and not DDOS protection system. It can make a device stateful. **Bank to Consider** - DDOS mitigation system should provide comprehensive outbound / Inbound traffic blocking for C&C, malware drop points, bad reputation IP/Domain/URL traffic.	Please be guided by RFP
93	Annexure D-97	66	System should support anti-evasion mechanisms	Anti evasion is a function / feature of IPS **Bank to Consider** - System should support anti-evasion or anti-bot mechanisms	Line Item 97 of Annexure D should be read as,"System should support DDOS anti-evasion "
94	Point 132	67	Integration with RADIUS and TACACS+	Kindly share the details of the RADIUS and TACACS+ solution (vendor name & Model)	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
95	115	67	Solution must support TLS 1.3 management GUI	DDOS appliance managemnt console is accessed by Banks internal team and not exposed to Internet hence request Bank to modify the Caluse .. **Bank to Consider** - System must support SSH for CLI / Secure access (HTTPS) for Management GUI.	Line Item 97 of Annexure D should be read as,"Solution must support TLS 1.2 or above management GUI"
96	Annexure D-115	67	Solution must support TLS 1.3 management GUI	DDOS appliance managemnt console is accessed by Banks internal team and not exposed to Internet hence request Bank to modify the Caluse .. **Bank to Consider** - System must support SSH for CLI / Secure access (HTTPS) for Management GUI.	Line Item 97 of Annexure D should be read as,"Solution must support TLS 1.2 or above management GUI"
97	62. Annexure G – Indicative Commercial Bid	73	Bank may procure additional mitigation/scrubbing licences during the contract period at the discovered cost.	request you to kindly reduce the price validity to procure mitigation/scrubbing license to one year, viz a viz the entire contract period. Or Based on the request from bank to purchase additional licenses, bidder will provide the prices at that time.	Please be guided by RFP.
98	Pre-Contract Integrity Pact - Fall Clause	103	Annexure N – Pre-Contract Integrity Pact 10. Price Fall Clause The Bidder undertakes that it has not supplied /is not supplying same or similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry /Department of the Government of India or PSUs during the currency of the contract and if it is found at any stage that same or similar product /Systems or Subsystems was supplied by the Bidder to any other Ministry /Department of the Government of India or a PSU or any Public Sector Bank at a lower price during the currency of the contract, then that very price will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Buyer, if the contract has already been concluded".	NTT Comment: We agree to execute the Integrity Pact. However, we request that the Fall Clause is removed from the Integrity Pact. Please note that prices quoted are based on several factors, including quantity, location of delivery, dollar rates, discounts received from OEMs and other contractual risks. For all practical purposes, we request deletion of the Fall Clause from the Integrity Pact. We also wish to bring to your notice, that by way of the Central Vigilance Commission (CVC) issued a Circular dated 13.01.2017, formulating standard operating procedure for adoption of Integrity Pact and the same does not include Fall Clause as an essential ingredient of the Pact.	Please be guided by RFP.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
99	General		The purpose-built appliance/solution should be able to seamlessly integrate and should support cloud signal with at least 4 Service Providers DDoS scrubbing centres services in INDIA.	DDOS on-premise solution provides real time protection against State exhaustion and application layer attack. During volumetric attack the on-premise solution should signal to upstream ISP based scrubbing centre for initiating mitigation automatically. It should communicate the victim prefix with the ISP's scrubbing centre so that mitigation can be triggered automatically. It is important that the DDOS solution deployed on-premise should get integrated with most of the ISP's in India, for automatic scrubbing centre mitigation trigger.	Please be guided by RFP.
100	General		The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and should support STIX & TAXII format integration with external security intelligence feeds	DDOS mitigation system should also block outbound malicious communication. It should stop infected hosts from communicating with external malicious C&C, malware drop points, Rogue IP's/Domains. The DDOS vendor should provide its own threat intelligence feed to block such outbound malicious traffic, at the same time should support third party threat feeds in industry standard STIX & TAXII format.	Please be guided by RFP.
101	General		DDOS Appliance should have an inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL/ Hash / domain / IP address / subnet)	DDOS appliance inspecting the threatfeed can help organisations to block the know attacks at the perimeter. DDOS solution at the perimeter of the network in inline deployment mode is the most appropriate place to enforce inbound and outbound IOC's. Hence it is important that DDOS mitigation appliance should have high IOC's count support for blocking.	Please be guided by RFP.
102	General			We suggest that bank should consider OEM eligibility criteria as well; apart from bidder eligibility criteria. Proposed OEM's on-premises Anti DDoS solution should have been procured by 3 (PSU /Private) Banks during last 5 years each of minimum 10 Gbps. An email confirmation from bank employee or PO have to be submitted with RFP response.	**Read clause as,** "Bidder should have implemented anti-DDOS services devices in at least two corporates out of which one should be a BFSI/ RBI/NPCI (excluding RRB and Co-operative Bank) during last 5 years. (Supporting document - Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter and/or Certificate of completion of the work). Proposed Appliance (make) should be deployed in atleast three BFSI/RBI/NPCI."

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response
103	General			**Bank to Consider** - Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off in Country.	Clause no. 53 should be read as: "Spares for the hardware/software offered should be available for at least 5 years from the date of project sign off at market and should not become end of life. RMA for the hardware/software offered should be available in bank premises within 8 hours of appliance failure after raising the ticket."
104	General			1.Packets per second (PPS) is one of the most important measurements to consider when planning a DDoS defense strategy and evaluating solutions. Protocol or network-layer DDoS attacks send large numbers of packets to targeted network infrastructures and infrastructure management tools. These protocol attacks include SYN floods and Smurf DDoS, among others, and their size is measured in packets per second (PPS). On a Gigabit link, for example, you can have anywhere from tens of thousands to millions of packets. In DDoS, an attacker's strategy is asynchronous, meaning the attacker attempts to do as little work as possible while making their target do a lot of work. Therefore, attackers tend to use smaller packets and force the target to respond with larger packets in response, which drains the target's resources. Smallest packets commonly seen on networks is a TCP ACK packet. TCP ACK packet has a 20 byte IP header and a 20 byte TCP header, adding up to 40 bytes. Because this is smaller than ethernet's minimum payload size of 46 bytes, it is automatically padded prior to transmission to bring it up to size. It is then wrapped with a 14 byte header and 4 byte CRC, to give the minimum ethernet frame size of 64 bytes When transmitted, each packet must also be preceded by a 7-byte preamble and 1-byte start-of-frame delimiter and must be followed by an inter-frame gap of at least 12 bytes. This makes the smallest transmission in ethernet effectively 84 bytes. Calculate the maximum packet rate of 84 bytes on a 10G link: 10Gbps / (84 bytes * 8 bits) = 14.88Mps	Please be guided by RFP
105	76	59 (123)	Proposed solution should have centralized management system.		**Please read the clause as,**"Proposed solution should have centralized management system, Hardware for management server shall be provided by Bank while Bidder has to provide the licenses "