



## **Corrigendum 1 - dated 05-10-2026**

**Request for Proposal (RFP) for Supply, Installation, Testing and Commissioning (SITC) of Anti-DDoS Appliance Solution with Comprehensive Onsite Warranty for Gujarat Security Operations Center at Gujarat State Data Centre (GSDC) , Gandhinagar (GEM/2026/B/7905368 Dated: 26.08.2026)**

Please find the pre-BID queries response and Corrigendum dated 05/10/2026

For more details visit <https://gil.gujarat.gov.in/>

## 1. Preamble

This Corrigendum is issued by Gujarat Informatics Limited (GIL), acting as the Bidding Agency on behalf of the Gujarat Security Operations Center (GSOC), Directorate of ICT & e-Governance, Science & Technology Department (DST), Government of Gujarat, pursuant to the Pre-Bid Meeting held in connection with the above referenced Request for Proposal (RFP).

In light of queries and clarifications received from prospective bidders during the Pre-Bid stage, the following amendments, clarifications, and modifications are hereby made to the original RFP document. This Corrigendum supersedes the corresponding provisions in the original RFP and shall form an integral part thereof. All other terms and conditions of the original RFP shall remain unchanged and in full force.

## 2. Amendments / Revisions to the RFP

As per Annexure-A and corrigendum.

## 3. Revised Implementation Timeline (Section 8.4)

The following table supersedes the Implementation Timeline table in Section 8.4 (Page 29) of the original RFP in its entirety:

| Sr. | Milestone                                                                                                                   | Timeline (from GeM Contract Date) |
|-----|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| 1   | Kick Off Meeting                                                                                                            | Within 1 week                     |
| 2   | Submission of HLD / LLD / Implementation Plan                                                                               | Within 4 weeks                    |
| 3   | Hardware delivery at DC                                                                                                     | Within 8 weeks                    |
| 4   | Installation, cabling, racking at DC; Configuration, integration, and baseline tuning                                       | Within 10 weeks                   |
| 5   | UAT and performance validation; Final Acceptance Test sign-off; SOP documentation and Go-Live with Onsite Training for team | Within 12 weeks                   |

## 4. Revised Penalty for Delay in Delivery of Solution and Services (Section 7.1)

The following table supersedes the "PENALTY FOR DELAY IN DELIVERY OF SOLUTION and SERVICES" section under Section 7.1 (Page 26) of the original RFP in its entirety:

| Sr. | SLA & Penalty Requirement                                                                                                                                        |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Delay in submission of HLD/LLD beyond timeline: 0.05% of Contract Value per week                                                                                 |
| 2   | Delay in Hardware delivery, installation and configuration with baseline tuning beyond timeline: 0.5% of Total Contract Value per week or part thereof (max 10%) |
| 3   | Delay in FAT beyond timeline: 0.5% of Total Contract Value per week or part thereof (max 10%)                                                                    |
| 4   | Delivery & installation and FAT penalties capped at 10% of total Contract Value                                                                                  |
| 5   | Quarterly penalties capped at 25% of quarterly charges                                                                                                           |

## 5. Payment Schedule

| Sr. | Stage                                                                                                                   | Payment | Condition                                                       |
|-----|-------------------------------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------|
| 1   | Submission of HLD / LLD / Implementation Plan, Hardware delivery at DC                                                  | 50%     | hardware, software, licenses delivery                           |
| 2   | Installation, cabling, racking at DC, Configuration, integration, and baseline tuning                                   | 30%     | Installation, configuration, integration with existing solution |
| 3   | UAT and performance validation, Final Acceptance Test sign-off, Onsite Training for team, SOP documentation and Go-Live | 20%     | Final Acceptance test passed, SOP documentation & Training      |
| 4   | 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges                                                | -       | in 20 equal instalments at the end of every Quarter.            |

Note: No change in Price Bid schedule and note conditions.

## 6. Additional Terms

- 1) Additional: If after the award of the contract the Bidder fails for Kick Off Meeting within SLA and to furnish the Performance Bank guarantee within fifteen (15) working days with working schedule as per the tender requirements & if the operation is not started within fifteen (15) working days after submission of P.B.G. as mentioned, GoG/GIL reserves the right to cancel the contract and apply all remedies available to him under the terms and conditions of this contract.
- 2) Additional: The date on which final acceptance Test (FAT) is completed shall be deemed to be date of successful commission of the equipment. Any delay by the successful Bidder in commissioning of equipment shall render the bidder liable to the imposition of appropriate liquidated damages.
- 3) Clause 4.2.5 following sub para stands removed:

“If the solution does not meet the required specifications or has significant discrepancies: The tenderer maintains the right to nullify the entire contract. Any amount paid at this point would be recovered from the PBG (performance Bank Guarantee) In such a case, the SELECTED BIDDER must remove their equipment at their own expense and risk”

- 4) Clause 4.2.5 following para added:

In the event of failure by the Successful Bidder to fulfill any of the requirements, obligations, deliverables, or terms and conditions of the Contract, the Government of Gujarat/GIL shall have the right to terminate or cancel the Contract. Any amount payable or recoverable from the Successful Bidder arising from such failure, including penalties, Liquidated Damages (LD), or other contractual dues, may be recovered from the Performance Bank Guarantee (PBG), without prejudice to any other rights and remedies available to the Government of Gujarat/GIL under the Contract or applicable law. GOG/GIL also reserves the right to blacklist such bidder from participating in future tenders if sufficient cause exists.

| Sr. | RFP Clause / Section                      | Existing Clause (As Issued)                                                                                                                                                                                                                                                                                                                                                                                                                           | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Eligibility Criteria<br>Page 8            | <p>The bidder should have experience in Supply, Installation, Testing and Commissioning (SITC) of Anti-DDoS solution. The following work order value criteria must be met in the last three financial years as on bid submission date (any one option):</p> <p>One work order having value of Rs. 16 Cr or</p> <p>Two work order, each work order having value of Rs. 10 Cr or</p> <p>Three work order, each work order having value of Rs. 08 Cr</p> | <p>Since Anti-DDoS is a specialized OEM-driven security solution, we request that the experience of the proposed OEM may also be considered for fulfilling the bidder's PQ experience criteria, provided the bidder is an authorized partner of the OEM and submits valid supporting documents.</p> <p>Justification:<br/>The technical capability, solution architecture, deployment expertise, and product performance of an Anti-DDoS solution are primarily dependent on the OEM's technology and implementation experience. Considering OEM experience will encourage wider participation while ensuring the availability of proven Anti-DDoS expertise.</p> | <p>2. Eligibility Criteria point 4. clause revised: The bidder should have experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution / Anti-DDoS solution as a part of cyber security solution in last three financial years.</p> <ul style="list-style-type: none"> <li>• One work order having value of Rs. 13 Cr or</li> <li>• Two work order, each work order having value of Rs. 10 Cr or</li> <li>• Three work order, each work order having value of Rs. 7 Cr.</li> </ul> |
| 2   | Section 4.1 — Broad Scope                 | Integration with SDC's existing network infrastructure: upstream routers, core switches, firewalls, load balancers                                                                                                                                                                                                                                                                                                                                    | Please share make/model and OS version details of existing upstream routers, core switches, firewalls, load balancers, and SIEM platform, along with current internet bandwidth/uplink capacity, to enable accurate solution design and BoM sizing.                                                                                                                                                                                                                                                                                                                                                                                                               | if require bidder may conduct site visit to understand existing infra.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 3   | Section 4.1 — Broad Scope                 | BGP peering configuration with SDC's 2 upstream ISPs for traffic diversion                                                                                                                                                                                                                                                                                                                                                                            | Please confirm whether ISP coordination, BGP session provisioning, and any associated ISP-side charges for scrubbing/diversion service will be arranged and borne by GIL/SDC, or fall within the bidder's scope.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 4   | Section 4.1 — Broad Scope                 | Integration with SDC's SIEM solution for log forwarding                                                                                                                                                                                                                                                                                                                                                                                               | Please confirm the SIEM platform/vendor in use at SDC and whether any professional services/licensing on the SIEM side (outside the DDoS OEM) will be arranged by GIL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Onprem SIEM solution is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 5   | Section 5.1, Sr.1 — Hardware Architecture | Purpose-built appliance with dedicated ASIC/NPU/FPGA; NOT a general-purpose x86 COTS server                                                                                                                                                                                                                                                                                                                                                           | <p>This clause restricts participation to OEMs using custom ASIC/NPU/FPGA architecture only, and excludes modern high-performance x86/DPU-based appliances that also achieve line-rate 100 Gbps mitigation. Request this be made more technology-neutral.</p> <p>Suggestion: Request the clause be revised to: 'Purpose-built security appliance (ASIC/NPU/FPGA or high-performance multi-core/DPU architecture) demonstrated to deliver line-rate 100 Gbps mitigation without performance degradation, to allow wider OEM participation</p>                                                                                                                      | Section 5.1, Sr.1 — Hardware Architecture clause revised to : Purpose-built inline DDoS mitigation appliance engineered for high-speed packet processing. The solution must utilize an optimized, stateless packet-processing architecture or hardware acceleration. It should not be general purpose platform and should not be part of UTM or load balancer                                                                                                                                              |
| 6   | Section 5.1, Sr.10-11 — Interfaces        | 16 x 10GigE bypass ports (LR/SR fiber) PLUS minimum 16 x 10GE/25GE SFP28 ports for management/monitoring (i.e., 32 ports total)                                                                                                                                                                                                                                                                                                                       | Request confirmation that port requirement may be met via a single chassis or a stacked/clustered configuration achieving equivalent aggregate ports and 100 Gbps throughput; request actual site fiber-run distances to finalize LR/SR mix                                                                                                                                                                                                                                                                                                                                                                                                                       | Section 5.1 Revised clauses: 10. Specifically mandates 16 x 10 GigE bypass ports (SR) fiber ports, and hot-swappable dual power supplies<br>11. minimum 16 x 10GE/25GE SFP28 ports for management and monitoring. additionally, 2 x 10G copper out of band management ports.<br>Port requirement must be met via Single Chassis configuration.                                                                                                                                                             |
| 7   | Section 5.3, Sr.2 — Real-Time Detection   | Detection-to-mitigation time: maximum 18 seconds; desirable < 10 seconds                                                                                                                                                                                                                                                                                                                                                                              | Please clarify whether this 18-second SLA applies uniformly to all attack types (including sophisticated L7/behavioral attacks that inherently require longer baselining) or only to signature-based/volumetric attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                          | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                                                                                                                                                                                                     |

| Sr. | RFP Clause / Section                                                                                              | Existing Clause (As Issued)                                                                                                                                                                                          | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                                                                                                                                |
|-----|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8   | Section 5.1 Sr.7 vs 5.2.3 Sr.2                                                                                    | SSL/TLS Connections per Session: Minimum 100 KCPS (Sec 5.1); TLS inspection throughput minimum 160 KCPS (Sec 5.2.3)                                                                                                  | These two SSL/TLS-related throughput figures appear in different sections with different values. Please clarify whether both apply simultaneously and to which specific function each figure corresponds (session setup rate vs inspection throughput).                                                                                                                                                                                                                                                                                                                                                                           | Section 5.2.3. Sr, 2 revised: SSL/TLS Decryption for DDoS. "Hardware-accelerated or TLS proxy based TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                                                                                                                         |
| 9   | Section 5.7, Sr.1 — Certification                                                                                 | Common Criteria (CC) EAL2+ or higher, mandatory, CCRA-recognized certificate                                                                                                                                         | Please confirm whether CC EAL2 certification (without the '+') is acceptable, as EAL2+ is a less commonly certified level among global Anti-DDoS OEMs and may restrict competition.<br><br>Suggestion: Request the clause be relaxed to 'CC EAL2 or higher, CCRA-recognized' to allow broader OEM participation                                                                                                                                                                                                                                                                                                                   | As per RFP                                                                                                                                                                                                                                                                                                                                                               |
| 10  | Section 5.5, Sr.1 — CMS                                                                                           | CMS may be hardware appliance or virtual machine; must reside on-premises within state data centre                                                                                                                   | If CMS is proposed as a virtual machine, please confirm whether the underlying server/compute/hypervisor infrastructure will be provided by GIL/SDC or must be supplied by the bidder as part of the solution.                                                                                                                                                                                                                                                                                                                                                                                                                    | As per RFP. Bidder has to provide all the required hardware/software and licenses to complete the solution and RFP requirement.                                                                                                                                                                                                                                          |
| 11  | Section 5.1 "Technical Specification". Requirement "Hardware Architecture" / ( Sr-1 / Page# 16)                   | Purpose-built DDoS mitigation appliance; NOT a general-purpose x86 COTS server repurposed for DDoS. Must have dedicated ASIC / NPU / FPGA for packet processing.                                                     | Prebid Query / Justification : The proposed DDoS mitigation solution shall not rely on fixed-function ASIC, router NPU, or FPGA-based processing as its primary detection and mitigation engine. It must use a fully programmable, purpose-built packet-processing architecture capable of supporting new attack countermeasures and protocol updates through software upgrades without requiring hardware replacement.<br><br>Change request : We request to remove this point and change clause as "Purpose-built DDoS mitigation appliance; NOT a general-purpose platform and should not be part of any UTM or Load Balancer" | Section 5.1, Sr.1 — Hardware Architecture clause revised to : Purpose-built inline DDoS mitigation appliance engineered for high-speed packet processing. The solution must utilize an optimized, stateless packet-processing architecture or hardware acceleration. It should not be general purpose platform and should not be part of UTM or load balancer            |
| 12  | Section 5.1 "Technical Specification". Requirement "External Intelligent Bypass / Fail-open" / ( Sr-1 / Page# 16) | Integrated hardware bypass (fail-open) capability to prevent network outage in case of appliance failure; must support optical and copper bypass. Additional hardware required should be bring by the bidder if any. | Prebid Query / Justification : Solution should support inbuilt fail open on all copper and fiber ports, this point is important to maintain high availability and to remove service disruption, and in case if vendor propose external fail open kit it have to be from same OEM.<br><br>Change request : Integrated hardware bypass (fail-open) capability to prevent network outage in case of appliance failure; must support optical and copper bypass. Additional hardware required should be bring by the bidder and external fail open kit should be from same OEM of proposed DDoS mitigation solution.                   | Section 5.1 Sr 1 revised: The solution shall provide integrated hardware fail-open/bypass functionality. Where an external hardware bypass is required for the offered interface configuration, the bidder shall provide an OEM-supplied or OEM-approved external hardware bypass solution, with documented interoperability with the proposed DDoS mitigation solution. |
| 13  | Section 5.1 "Technical Specification". Requirement "SSL/TLS Connection Per Session" / ( Sr-3 / Page# 16)          | Minimum 100 KCPS                                                                                                                                                                                                     | Prebid Query / Justification - Selective decryption is having Lower performance overhead: Processing capacity is reserved for high-risk or protected traffic instead of decrypting every TLS session.<br>Higher mitigation throughput: The appliance can handle more concurrent connections and attack traffic.<br><br>Change request : We request to change clause as "DDoS mitigation solution should support minimum 100 K SSL CPS with selective decrvption using TLS proxy"                                                                                                                                                  | Section 5.1 Sr. 7 revised: DDoS mitigation solution should support minimum 100 KCPS with decryption using TLS proxy or Hardware TLS acceleration                                                                                                                                                                                                                         |
| 14  | Section 5.1 "Technical Specification". Requirement "Network Interfaces" / ( Sr-11 / Page# 17)                     | Minimum 16 x 10GE/25GE SFP28 ports for management and monitoring.                                                                                                                                                    | Prebid Query / Justification: We do not need more than two out of band ports for management and monitoring.<br>Change request : We request to change clause as "minimum 2 x 1GE or 2 x 10GE copper out of band management ports"                                                                                                                                                                                                                                                                                                                                                                                                  | Section 5.1 revised Sr. 11. minimum 16 x <b>10GE/25GE</b> SFP28 ports for management and monitoring. additionally, 2 x 10G copper out of band management ports.                                                                                                                                                                                                          |
| 15  | Section 5.2 2 "Technical Specification". Requirement "Protocol Attacks" / ( Sr-2 / Page# 18)                      | Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioral fingerprinting, CAPTCHA challenge, rate limiting per source IP"                                                       | Prebid Query / Justification: CAPTCHA Challenge is older authentication method and is intrusive, also will make DDoS mitigation solution stateful.<br><br>Change request : We request to remove CAPTCHA and change clause as "Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioral fingerprinting, rate limiting per source IP"                                                                                                                                                                                                                                                         | Section 5.2 2 Sr. 2 Revised: HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, rate limiting per source IP                                                                                                                                                                                                                                                    |

| Sr. | RFP Clause / Section                                                                            | Existing Clause (As Issued)                                                                                                                                         | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Responses                                                                                                                                                                                                                                                                                                             |
|-----|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16  | Section 5.2 2 "Technical Specification". Requirement "Protocol Attacks" /<br>( Sr-6 / Page# 18) | Hardware TLS acceleration for inspection; TLS handshake rate limiting                                                                                               | Prebid Query / Justification: Modern DDoS mitigation solution use TLS proxy for TLS 1.3 PFS decryption using TLS fingerprinting and selective decryption. Selective decryption helps in achieving higher performance.<br><br>Change request : We request to change clause as "Hardware TLS acceleration or Proxy based TLS inspection; TLS handshake rate limiting"                                                                                                                       | Section 5.2 2 Sr 6 revised: Hardware TLS acceleration or Proxy based TLS inspection; TLS handshake rate limiting                                                                                                                                                                                                      |
| 17  | Section 5.2.3. "Technical Specification". SSL/TLS Decryption for DDoS /<br>( Sr-2 / Page# 18)   | SSL/TLS Decryption for DDoS. "Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"     | Prebid Query / Justification: Modern DDoS mitigation solution use TLS proxy for TLS 1.3 PFS decryption using TLS fingerprinting and selective decryption. Selective decryption helps in achieving higher performance.<br><br>Change request : We request to change clause as "Hardware-accelerated or Proxy based TLS 1.2 ECDHE and TLS 1.3 PFS decryption for application-layer inspection; TLS inspection throughput Minimum 100 K CPS using selective decryption / TLS fingerprinting" | Section 5.2.3. Sr, 2 revised: SSL/TLS Decryption for DDoS. "Hardware-accelerated or TLS proxy based TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                                                                      |
| 18  | Section 5.2.3. "Technical Specification". API Protection /<br>( Sr-5 / Page# 18)                | Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection                                                                                               | Prebid Query / Justification: Asked feature will make DDoS mitigation solution stateful and prone to state exhaustion attacks.<br><br>Change request : We request to change point as "System should have capability for source rate limit on URI or REGEX of URI"                                                                                                                                                                                                                         | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                |
| 19  | Section 5.3. "Technical Specification". Real-Time Attack Detection. /<br>( Sr-2 / Page# 19)     | Detection-to-mitigation time: maximum 18 seconds for automated signature activation; desirable ≤ 10 seconds.                                                        | Change request : We request to change clause as "Detection-to-mitigation time: maximum 18 seconds for automated signature / countermeasure activation; desirable ≤ 10 seconds."                                                                                                                                                                                                                                                                                                           | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                |
| 20  | Section 5.3. "Technical Specification". Signature-Based Detection /<br>( Sr-3 / Page# 19)       | Pre-built library of DDoS attack signatures; real-time signature updates from OEM threat intelligence feed (cloud-connected or offline update) at ≤4-hour interval. | Change request : We request to change clause as "Pre-built library of DDoS attack signatures / reputation feed; real-time signature / reputation feeds updates from OEM threat intelligence feed (cloud-connected or offline update) at ≤4-hour interval. System should have support up to 10 Million IoC's and should integrate on STIX / TAXI with third party Threat Intelligence Platform "                                                                                           | Section 5.3. Sr. 3 revised: Pre-built library of DDoS attack signatures/reputation feed; real-time signature/reputation feed updates from OEM threat intelligence feed (cloud-connected or offline update) at ≤4-hour interval. Preferably support integration with Third party intelligence using STIX/TAXI for IOCs |
| 21  | Section 5.3. "Technical Specification". False Positive Rate /<br>( Sr-3 / Page# 19)             | Bidder to demonstrate false positive rate of < 1% in reference deployment.                                                                                          | Prebid Query / Justification": Asked feature need more clarity in terms of false positive generation on DDoS mitigation engine along with classification of False Positive rate.                                                                                                                                                                                                                                                                                                          | Clause Removed                                                                                                                                                                                                                                                                                                        |
| 22  | Section 5.6. "Technical Specification". Reporting Requirement /<br>( Sr-4 / Page# 22)           | Reports suitable for regulatory audit: ISO 27001, Cybersecurity framework compliance posture.                                                                       | Change request : We request to change clause as "Reports suitable for regulatory audit: as per Cybersecurity framework compliance posture."                                                                                                                                                                                                                                                                                                                                               | Section 5.6. Sr. 4 revised: Reports suitable for regulatory audit and Cybersecurity framework compliance posture.                                                                                                                                                                                                     |
| 23  | Section 7.1 Appliance Uptime & Availability<br>( Sr-10 / Page# 26)                              | Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 7 working days                                                                                   | Justification: Hotfix/patch/vulnerability deployment depends on severity of issue.<br><br>Change request: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 15 working days or any work around.                                                                                                                                                                                                                                                                          | 7.1 Appliance Uptime & Availability Sr10 clause revised: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 14 days                                                                                                                                                                                   |

| Sr. | RFP Clause / Section                                                          | Existing Clause (As Issued)                                                                                                                                                                                                                                                                                                | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 24  | Section 4.2.5 Implementation/Operation (Page# 23)                             | OEM/ISV to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc.     | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "OEM/ISV/Bidder to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM/ISV/Bidder every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc." | Section 4.2.5 clause revised: OEM/Top tier OEM authorized Partner to assess and certify the implementation, hardening and configuration of the solution. Onsite Health check should be carried out by OEM/Top tier OEM authorized Partner every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM/Top tier OEM authorized Partner itself of CPU utilization, database activities, OS status, etc. |
| 25  | Section 4.2.5 Implementation/Operation (Page# 23)                             | The OEM shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue. | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "The OEM/Bidder shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/Bidder/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue." | Section 4.2.5 clause revised: The bidder's team shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/bidder's team suitable rectification steps/proper Support shall be provided by OEM till eradication of the issue.                                                                                 |
| 26  | Section 8.4 Delivery & Implementation Timeline (Sr-2 / Page# 29)              | Hardware delivery at DC: Within 2 - 4 weeks                                                                                                                                                                                                                                                                                | Justification: Globally the current lead time for hardware delivery is about 10 weeks, so we request to change this as follows.<br>Change request: Hardware delivery at DC: Within 8 - 10 weeks                                                                                                                                                                                                                                                                                                                      | See corrigendum point 3                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 27  | 2. Eligibility Criteria (Page# 9)                                             | OEM Should have supplied Anti-DDoS solution having value of Rs. 50 cr. work order should be available in the last three financial years as on bid submission.                                                                                                                                                              | Justification: Since as per point # 4 on page 8 bidder is required to have single work order with value of 16 cr, OEM should have single work order to be twice the value of bidder. So, we request to change this clause as follows.<br><br>Change request: OEM Should have supplied Anti-DDoS solution having value of Rs. 32 cr. single work order should be available in the last three financial years as on bid submission.                                                                                    | 2. Eligibility Criteria Sr 4 revised: OEM Should have supplied Anti-DDoS solution having value of Rs. 30 cr. work order should be available in the last three financial years as on bid submission.                                                                                                                                                                                                                                                     |
| 28  | 8.4 Delivery & Implementation Timeline / Payment Schedule (Sr - 4 / Page# 30) | 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: in 20 equal instalments at the end of every Quarter.                                                                                                                                                                                             | Justification: We request to change this clause as follows:<br><br>Change request: 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: Yearly advance                                                                                                                                                                                                                                                                                                                                          | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Sr. | RFP Clause / Section                                                                                                                       | Existing Clause (As Issued)                                                                                                                                     | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Responses                                                                                                                                                                                                                                                    |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. "On-Demand / Out-of-Path Scrubbing" /<br>( Sr-2 / Page# 20) | BGP diversion: traffic rerouted to appliance scrubbing center during detected attacks; clean traffic re-injected via GRE / IPIP tunnel or policy-based routing. | Prebid Query / Justification: Scrubbing of DDoS traffic should be done in backbone of upstream service provider (ISP) when DDoS attack become volumetric and chokes last mile. On Premise DDoS mitigation solution should send cloud signal to scrubber in backbone of Service Provider for handoff of traffic. References for clause in Public RFP's like: SBI, PNB, RBI, LIC, IDBI etc.<br><br>Change request :<br><br>We request to change spec as "On Premise DDoS mitigation solution should send Cloud signal to upstream ISPs who is providing anti-DDoS cloud service clean pipe for very large DDoS attack mitigation.<br>The signaling should be native without any REST API and must be supported with the following ISPs (SIFY, TATA, AIRTEL but not limited to) or MSSPs of the following ISPs (SIFY, TATA, AIRTEL but not limited to) in India. No data should be required to be routed to any third party cloud provider.<br>No Data/information shall leave Indian Sub-continent at any point and shall adhere to MEITY, RBI and GOI Guidelines at all time during market practices for | Clause Revised to:<br>The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.4 Sr 2 via cloud signaling to upstream ISP. At any point of time Data/information must not leave india . |
| 30  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Surgical Mitigation /<br>( Sr-3 / Page# 20)                 | Granular per-flow mitigation capability: ability to drop attack flows while passing legitimate flows from same source IP; not blunt IP-block based.             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | As per RFP                                                                                                                                                                                                                                                   |
| 31  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Blackholing / RTBH /<br>( Sr-4 / Page# 20)                  | Remote Triggered Black Hole (RTBH) support via BGP for extreme volumetric events as last resort.                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Clause Revised to: The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.4 Sr 4 via cloud signaling to upstream ISP.                                                                 |
| 32  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Rate Limiting /<br>( Sr-5 / Page# 20)                       | Granular rate limiting: per source IP, per destination IP, per subnet, per protocol, per port — independently configurable.                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | As per RFP                                                                                                                                                                                                                                                   |
| 33  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Geo-based Filtering /<br>( Sr-6 / Page# 20)                 | Country/region-based traffic filtering with country-level block/rate-limit capability. GeoIP database must be updated at minimum monthly.                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | As per RFP                                                                                                                                                                                                                                                   |

| Sr. | RFP Clause / Section                                                                                                               | Existing Clause (As Issued)                                                                                          | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. ACL / Blacklist / Whitelist /<br>( Sr-7 / Page# 20) | Dynamic and static ACL support: blacklist and whitelist IP ranges, autonomous systems (AS numbers), and CIDR blocks. |                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 35  | Section 5.5 "Technical Specification".Management & Visibility Requirements                                                         | Support Netflow v9 / IPFIX /sflow for traffic visibility to external flow collectors / analyzers                     | Prebid Query / Justification: Mention requirement is for On Demand DDoS Mitigation solution which ingest Flow record detect DDoS and redirect traffic to scrubber through BGP route diversion. Requirement is here for Inline DDoS mitigation solution.<br>Change Request: We request to remove this specification, this do not align with Inline solution. | Clause Revised to: The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.5 Sr 9 via cloud signaling to upstream ISP.                                                                                                                                                                                                                                                            |
| 36  | Clause 2,Page no. 8                                                                                                                | Eligibility Criteria- Order value reference                                                                          | Kindly consider the experience and order value credentials of the Bidder or OEM for this eligibility criteria.                                                                                                                                                                                                                                              | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 37  | Clause 4.2.5, Implementation/Operation, Page 13                                                                                    | OEM Certified Manpower Operations Team                                                                               | Kindly clarify the minimum number of onsite resources required during the 5-year support period.                                                                                                                                                                                                                                                            | Minimum 1 manpower.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 38  | Clause 4.2.5, Page 13-14                                                                                                           | OEM Health Checks                                                                                                    | Kindly clarify whether half-yearly health checks and annual assessments can be performed remotely or require onsite visits.                                                                                                                                                                                                                                 | Section 4.2.5 clause revised: OEM/Top tier OEM authorized Partner to assess and certify the implementation, hardening and configuration of the solution. Onsite Health check should be carried out by OEM/Top tier OEM authorized Partner every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM/Top tier OEM authorized Partner itself of CPU utilization, database activities, OS status, etc. |
| 39  | Clause 5.3, Detection Requirements, Page 19                                                                                        | False Positive Rate <1%                                                                                              | Kindly provide methodology to measure and validate false-positive SLA compliance.                                                                                                                                                                                                                                                                           | Clause Removed                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 40  | Clause 5.5, Management & Visibility, Page 20-21                                                                                    | SIEM Integration                                                                                                     | Kindly provide details of existing SIEM platform including OEM, version and integration interfaces available.                                                                                                                                                                                                                                               | Onprem SIEM solution is available, integrations will be standard. details will be provided to successful bidder.                                                                                                                                                                                                                                                                                                                                        |
| 41  | Clause 7.1, SLA, Page 25                                                                                                           | Solution Availability 99.95%                                                                                         | Kindly clarify the formula for SLA availability calculation and confirm whether planned maintenance windows are excluded.                                                                                                                                                                                                                                   | RFP already mentioned that availability 99.95% excluding planned downtime .                                                                                                                                                                                                                                                                                                                                                                             |
| 42  | Clause 7.2, FMS Support, Page 27                                                                                                   | Onsite Engineer Requirement                                                                                          | Kindly clarify whether onsite support is required on weekends, public holidays and beyond business hours.                                                                                                                                                                                                                                                   | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 43  | Clause 8.1, Warranty & AMC, Page 28                                                                                                | Hardware Replacement Obligation                                                                                      | Kindly confirm whether replacement with equivalent or higher-generation OEM model shall be acceptable if the proposed model becomes EOS/EOL during contract period.                                                                                                                                                                                         | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 44  | Clause 8.4, Payment Schedule, Page 29-30                                                                                           | Payment Terms                                                                                                        | Kindly clarify payment release timeline from invoice submission date after successful milestone completion. (e.g., 30 days/45 days/60 days).                                                                                                                                                                                                                | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 45  | Clause 8.4, Payment Schedule, Page 29-30                                                                                           | Payment Terms                                                                                                        | Kindly clarify whether O&M quarterly payments will be released in advance or in arrears after completion of each quarter.                                                                                                                                                                                                                                   | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 46  | Clause 8.4, Page 30-31                                                                                                             | O&M Cost Not Less Than 35%                                                                                           | Kindly clarify whether the 35% O&M value calculation shall be considered before GST or including GST.                                                                                                                                                                                                                                                       | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 47  | Section 8.3,Page 30                                                                                                                | PBG                                                                                                                  | Kindly clarify the exact validity period of PBG since the RFP states contract period plus six months as well as warranty period plus 180 days. Please confirm the final requirement.                                                                                                                                                                        | PBG: Of total contract value, valid for contract period + 6 months                                                                                                                                                                                                                                                                                                                                                                                      |
| 48  | Section 8.3,Page 30                                                                                                                | PBG                                                                                                                  | Kindly confirm whether PBG value can be proportionately reduced after successful completion of implementation and during the AMC/O&M period.                                                                                                                                                                                                                | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Sr. | RFP Clause / Section                                                                                              | Existing Clause (As Issued)                                                                                                                                                                                          | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                                                                                                                                |
|-----|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 49  | Section 5.1 "Technical Specification". Requirement "Hardware Architecture" / ( Sr-1 / Page# 16)                   | Purpose-built DDoS mitigation appliance; NOT a general-purpose x86 COTS server repurposed for DDoS. Must have dedicated ASIC / NPU / FPGA for packet processing.                                                     | Prebid Query / Justification : The proposed DDoS mitigation solution shall not rely on fixed-function ASIC, router NPU, or FPGA-based processing as its primary detection and mitigation engine. It must use a fully programmable, purpose-built packet-processing architecture capable of supporting new attack countermeasures and protocol updates through software upgrades without requiring hardware replacement.<br><br>Change request : We request to remove this point and change clause as "Purpose-built DDoS mitigation appliance; NOT a general-purpose platform and should not be part of any UTM or Load Balancer" | Section 5.1, Sr.1 — Hardware Architecture clause revised to : Purpose-built inline DDoS mitigation appliance engineered for high-speed packet processing. The solution must utilize an optimized, stateless packet-processing architecture or hardware acceleration. It should not be general purpose platform and should not be part of UTM or load balancer            |
| 50  | Section 5.1 "Technical Specification". Requirement "External Intelligent Bypass / Fail-open" / ( Sr-1 / Page# 16) | Integrated hardware bypass (fail-open) capability to prevent network outage in case of appliance failure; must support optical and copper bypass. Additional hardware required should be bring by the bidder if any. | Prebid Query / Justification : Solution should support inbuilt fail open on all copper and fiber ports, this point is important to maintain high availability and to remove service disruption, and in case if vendor propose external fail open kit it have to be from same OEM.<br><br>Change request : Integrated hardware bypass (fail-open) capability to prevent network outage in case of appliance failure; must support optical and copper bypass. Additional hardware required should be bring by the bidder and external fail open kit should be from same OEM of proposed DDoS mitigation solution.                   | Section 5.1 Sr 1 revised: The solution shall provide integrated hardware fail-open/bypass functionality. Where an external hardware bypass is required for the offered interface configuration, the bidder shall provide an OEM-supplied or OEM-approved external hardware bypass solution, with documented interoperability with the proposed DDoS mitigation solution. |
| 51  | Section 5.1 "Technical Specification". Requirement "SSL/TLS Connection Per Session" / ( Sr-3 / Page# 16)          | Minimum 100 KCPS                                                                                                                                                                                                     | Prebid Query / Justification - Selective decryption is having Lower performance overhead: Processing capacity is reserved for high-risk or protected traffic instead of decrypting every TLS session. Higher mitigation throughput: The appliance can handle more concurrent connections and attack traffic.<br><br>Change request : We request to change clause as "DDoS mitigation solution should support minimum 100 K SSL CPS with selective decryption using TLS proxy"                                                                                                                                                     | Section 5.1 Sr. 7 revised: DDoS mitigation solution should support minimum 100 KCPS with decryption using TLS proxy or Hardware TLS acceleration                                                                                                                                                                                                                         |
| 52  | Section 5.1 "Technical Specification". Requirement "Network Interfaces" / ( Sr-11 / Page# 17)                     | Minimum 16 x 10GE/25GE SFP28 ports for management and monitoring.                                                                                                                                                    | Prebid Query / Justification: We do not need more than two out of band ports for management and monitoring.<br>Change request : We request to change clause as "minimum 2 x 1GE or 2 x 10GE copper out of band management ports"                                                                                                                                                                                                                                                                                                                                                                                                  | Section 5.1 revised Sr. 11. minimum 16 x 10GE/25GE SFP28 ports for management and monitoring. additionally, 2 x 10G copper out of band management ports.                                                                                                                                                                                                                 |
| 53  | Section 5.2 2 "Technical Specification". Requirement "Protocol Attacks" / ( Sr-2 / Page# 18)                      | Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioral fingerprinting, CAPTCHA challenge, rate limiting per source IP"                                                       | Prebid Query / Justification: CAPTCHA Challenge is older authentication method and is intrusive, also will make DDoS mitigation solution stateful.<br><br>Change request : We request to remove CAPTCHA and change clause as "Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioral fingerprinting, rate limiting per source IP"                                                                                                                                                                                                                                                         | Section 5.2 2 Sr. 2 Revised: HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, rate limiting per source IP                                                                                                                                                                                                                                                    |
| 54  | Section 5.2 2 "Technical Specification". Requirement "Protocol Attacks" / ( Sr-6 / Page# 18)                      | Hardware TLS acceleration for inspection; TLS handshake rate limiting                                                                                                                                                | Prebid Query / Justification: Modern DDoS mitigation solution use TLS proxy for TLS 1.3 PFS decryption using TLS fingerprinting and selective decryption. Selective decryption helps in achieving higher performance.<br><br>Change request : We request to change clause as "Hardware TLS acceleration or Proxy based TLS inspection; TLS handshake rate limiting"                                                                                                                                                                                                                                                               | Section 5.2 2 Sr 6 revised: Hardware TLS acceleration or Proxy based TLS inspection; TLS handshake rate limiting                                                                                                                                                                                                                                                         |
| 55  | Section 5.2.3. "Technical Specification". SSL/TLS Decryption for DDoS / ( Sr-2 / Page# 18)                        | SSL/TLS Decryption for DDoS. "Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                      | Prebid Query / Justification: Modern DDoS mitigation solution use TLS proxy for TLS 1.3 PFS decryption using TLS fingerprinting and selective decryption. Selective decryption helps in achieving higher performance.<br><br>Change request : We request to change clause as "Hardware-accelerated or Proxy based TLS 1.2 ECDHE and TLS 1.3 PFS decryption for application-layer inspection; TLS inspection throughput Minimum 100 K CPS using selective decryption / TLS fingerprinting"                                                                                                                                         | Section 5.2.3. Sr, 2 revised: SSL/TLS Decryption for DDoS. "Hardware-accelerated or TLS proxy based TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                                                                                                                         |

| Sr. | RFP Clause / Section                                                                        | Existing Clause (As Issued)                                                                                                                                                                                                                                                                                                | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 56  | Section 5.2.3. "Technical Specification". API Protection /<br>( Sr-5 / Page# 18)            | Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection                                                                                                                                                                                                                                                      | Prebid Query / Justification: Asked feature will make DDoS mitigation solution stateful and prone to state exhaustion attacks.<br><br>Change request : We request to change point as "System should have capability for source rate limit on URI or REGEX of URI"                                                                                                                                                                                                                                                    | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                                                                                                                                                  |
| 57  | Section 5.3. "Technical Specification". Real-Time Attack Detection. /<br>( Sr-2 / Page# 19) | Detection-to-mitigation time: maximum 18 seconds for automated signature activation; desirable ≤ 10 seconds.                                                                                                                                                                                                               | Change request : We request to change clause as "Detection-to-mitigation time: maximum 18 seconds for automated signature / countermeasure activation; desirable ≤ 10 seconds."                                                                                                                                                                                                                                                                                                                                      | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                                                                                                                                                  |
| 58  | Section 5.3. "Technical Specification". Signature-Based Detection /<br>( Sr-3 / Page# 19)   | Pre-built library of DDoS attack signatures; real-time signature updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval.                                                                                                                                                       | Change request : We request to change clause as "Pre-built library of DDoS attack signatures / reputation feed; real-time signature / reputation feeds updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. System should have support up to 10 Million IoC's and should integrate on STIX / TAXI with third party Threat Intelligence Platform "                                                                                                                     | Section 5.3. Sr. 3 revised: Pre-built library of DDoS attack signatures/reputation feed; real-time signature/reputation feed updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. Preferably support integration with Third party intelligence using STIX/TAXI for IOCs                                                                                                                                  |
| 59  | Section 5.3. "Technical Specification". False Positive Rate /<br>( Sr-3 / Page# 19)         | Bidder to demonstrate false positive rate of < 1% in reference deployment.                                                                                                                                                                                                                                                 | Prebid Query / Justification": Asked feature need more clarity in terms of false positive generation on DDoS mitigation engine along with classification of False Positive rate.                                                                                                                                                                                                                                                                                                                                     | Clause Removed                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 60  | Section 5.6. "Technical Specification". Reporting Requirement /<br>( Sr-4 / Page# 22)       | Reports suitable for regulatory audit: ISO 27001, Cybersecurity framework compliance posture.                                                                                                                                                                                                                              | Change request : We request to change clause as "Reports suitable for regulatory audit: as per Cybersecurity framework compliance posture."                                                                                                                                                                                                                                                                                                                                                                          | Section 5.6. Sr. 4 revised: Reports suitable for regulatory audit and Cybersecurity framework compliance posture.                                                                                                                                                                                                                                                                                                                                       |
| 61  | Section 7.1 Appliance Uptime & Availability<br>( Sr-10 / Page# 26)                          | Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 7 working days                                                                                                                                                                                                                                          | Justification: Hotfix/patch/vulnerability deployment depends on severity of issue.<br><br>Change request: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 15 working days or any work around.                                                                                                                                                                                                                                                                                                     | 7.1 Appliance Uptime & Availability Sr10 clause revised: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 14 days                                                                                                                                                                                                                                                                                                                     |
| 62  | Section 4.2.5 Implementation/Operation<br>(Page# 23)                                        | OEM/ISV to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc.     | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "OEM/ISV/Bidder to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM/ISV/Bidder every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc." | Section 4.2.5 clause revised: OEM/Top tier OEM authorized Partner to assess and certify the implementation, hardening and configuration of the solution. Onsite Health check should be carried out by OEM/Top tier OEM authorized Partner every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM/Top tier OEM authorized Partner itself of CPU utilization, database activities, OS status, etc. |
| 63  | Section 4.2.5 Implementation/Operation<br>(Page# 23)                                        | The OEM shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue. | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "The OEM/Bidder shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/Bidder/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue." | Section 4.2.5 clause revised: The bidder's team shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/bidder's team suitable rectification steps/proper Support shall be provided by OEM till eradication of the issue.                                                                                 |

| Sr. | RFP Clause / Section                                                                                                                       | Existing Clause (As Issued)                                                                                                                                     | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Responses                                                                                                                                                                                           |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64  | Section 8.4 Delivery & Implementation Timeline<br>( Sr-2 / Page# 29)                                                                       | Hardware delivery at DC: Within 2 - 4 weeks                                                                                                                     | Justification: Globally the current lead time for hardware delivery is about 10 weeks, so we request to change this as follows.<br>Change request: Hardware delivery at DC: Within 8 - 10 weeks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | See corrigendum point 3                                                                                                                                                                             |
| 65  | 2. Eligibility Criteria<br>(Page# 9)                                                                                                       | OEM Should have supplied Anti-DDoS solution having value of Rs. 50 cr. work order should be available in the last three financial years as on bid submission.   | Justification: Since as per point # 4 on page 8 bidder is required to have single work order with value of 16 cr, OEM should have single work order to be twice the value of bidder. So, we request to change this clause as follows.<br>Change request: OEM Should have supplied Anti-DDoS solution having value of Rs. 32 cr. single work order should be available in the last three financial years as on bid submission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2. Eligibility Criteria Sr 4 revised: OEM Should have supplied Anti-DDoS solution having value of Rs. 30 cr. work order should be available in the last three financial years as on bid submission. |
| 66  | 8.4 Delivery & Implementation Timeline / Payment Schedule<br>( Sr - 4 / Page# 30)                                                          | 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: in 20 equal instalments at the end of every Quarter.                                  | Justification: We request to change this clause as follows:<br>Change request: 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: Yearly advance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | As per RFP                                                                                                                                                                                          |
| 67  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. "On-Demand / Out-of-Path Scrubbing" /<br>( Sr-2 / Page# 20) | BGP diversion: traffic rerouted to appliance scrubbing center during detected attacks; clean traffic re-injected via GRE / IPIP tunnel or policy-based routing. | Prebid Query / Justification: Scrubbing of DDoS traffic should be done in backbone of upstream service provider (ISP) when DDoS attack become volumetric and chokes last mile. On Premise DDoS mitigation solution should send cloud signal to scrubber in backbone of Service Provider for handoff of traffic. References for clause in Public RFP's like: SBI, PNB, RBI, LIC, IDBI etc.<br>Change request :<br>We request to change spec as "On Premise DDoS mitigation solution should send Cloud signal to upstream ISPs who is providing anti-DDoS cloud service clean pipe for very large DDoS attack mitigation.<br>The signaling should be native without any REST API and must be supported with the following ISPs (SIFY, TATA, AIRTEL but not limited to) or MSSPs of the following ISPs (SIFY, TATA, AIRTEL but not limited to) in India. No data should be required to be routed to any third party cloud provider.<br>No Data/information shall leave Indian Sub-continent at any point and shall adhere to MEITY, RBI and GOI Guidelines at all time during market practices for | Clause Revised to: The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.4 Sr 2 via cloud signaling to upstream ISP.        |
| 68  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Surgical Mitigation /<br>( Sr-3 / Page# 20)                 | Granular per-flow mitigation capability: ability to drop attack flows while passing legitimate flows from same source IP; not blunt IP-block based.             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | As per RFP                                                                                                                                                                                          |

| Sr. | RFP Clause / Section                                                                                                               | Existing Clause (As Issued)                                                                                                               | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                | Responses                                                                                                                                                                                    |
|-----|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 69  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Blackholing / RTBH /<br>( Sr-4 / Page# 20)          | Remote Triggered Black Hole (RTBH) support via BGP for extreme volumetric events as last resort.                                          |                                                                                                                                                                                                                                                                                                                                                             | Clause Revised to: The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.4 Sr 4 via cloud signaling to upstream ISP. |
| 70  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Rate Limiting /<br>( Sr-5 / Page# 20)               | Granular rate limiting: per source IP, per destination IP, per subnet, per protocol, per port — independently configurable.               |                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                                                                                                                                                   |
| 71  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. Geo-based Filtering /<br>( Sr-6 / Page# 20)         | Country/region-based traffic filtering with country-level block/rate-limit capability. GeoIP database must be updated at minimum monthly. |                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                                                                                                                                                   |
| 72  | Section 5.4. "Technical Specification". Traffic Scrubbing & Mitigation Method. ACL / Blacklist / Whitelist /<br>( Sr-7 / Page# 20) | Dynamic and static ACL support: blacklist and whitelist IP ranges, autonomous systems (AS numbers), and CIDR blocks.                      |                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                                                                                                                                                   |
| 73  | Section 5.5 "Technical Specification".Management & Visibility Requirements                                                         | Support Netflow v9 / IPFIX /sflow for traffic visibility to external flow collectors / analyzers                                          | Prebid Query / Justification: Mention requirement is for On Demand DDoS Mitigation solution which ingest Flow record detect DDoS and redirect traffic to scrubber through BGP route diversion. Requirement is here for Inline DDoS mitigation solution.<br>Change Request: We request to remove this specification, this do not align with Inline solution. | Clause Revised to: The DDoS solution MUST be deployed in a primary Inline (Always-On) architecture for real-time traffic scrubbing and section 5.5 Sr 9 via cloud signaling to upstream ISP. |

| Sr. | RFP Clause / Section               | Existing Clause (As Issued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 74  | 2. Eligibility Criteria; page no 8 | <p>Eligibility Criteria:<br/>The bidder should have experience in Supply, Installation, Testing and Commissioning (SITC) of Anti-DDoS solution. The following work order value criteria must be met in the last three financial years as on bid submission date (any one option):<br/># One work order having value of Rs. 16 Cr or<br/># Two work order, each work order having value of Rs. 10 Cr or<br/># Three work order, each work order having value of Rs. 08 Cr<br/>All work orders / contracts should be in the name of the bidder</p> | <p>We humbly request the Purchaser to kindly reconsider and relax the prescribed work order values under the experience criteria for SITC of Anti-DDoS Solution. Anti-DDoS solutions are typically implemented as a component of larger Cybersecurity, network security, data centre, or infrastructure projects, and therefore the standalone value attributable to Anti-DDoS deployments may not meet the stipulated thresholds despite successful execution of similar assignments.</p> <p>In order to encourage broader participation of capable and experienced bidders and to enhance competition without compromising the project's objectives, we request the Purchaser to consider revising the criteria as follows:</p> <p>One work order having value of Rs. 16 3.00 Cr; or<br/>Two work orders, each work order having value of Rs. 10 1.75 Cr; or<br/>Three work orders, each work order having value of Rs. 08 1.25 Cr.</p> <p>Alternatively, bidders may be allowed to submit experience credentials where Anti-DDoS solution formed part of a larger network security, Cybersecurity, SOC, data centre, cloud, or ICT infrastructure project, with supporting documentary evidence.</p> <p>This modification will enable participation from a wider pool of qualified bidders having relevant implementation experience, thereby fostering healthy competition and ensuring optimum value for the Purchaser.</p> <p>Key Reasons for Seeking Reduction in Work Order Value<br/>Anti-DDoS is normally a component and not a standalone project, therefore dedicated work orders of such high values are uncommon.<br/>The prescribed thresholds are disproportionately high compared to the market value of Anti-DDoS deployments.<br/>Qualified bidders may get excluded despite having successfully implemented similar solutions as part of larger Cybersecurity engagements.<br/>Broader participation increases competition, resulting in better commercial outcomes for the department.<br/>Technical capability is not linked solely to project value; successful execution of multiple relevant deployments adequately demonstrates competency.<br/>Relaxation aligns with prevailing government procurement practices, where experience of similar technology components executed within larger projects is generally accepted.</p> | <p>2. Eligibility Criteria point 4. clause revised: The bidder should have experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution / Anti-DDoS solution as a part of cyber security solution in last three financial years.</p> <ul style="list-style-type: none"><li>• One work order having value of Rs. 13 Cr or</li><li>• Two work order, each work order having value of Rs. 10 Cr or</li><li>• Three work order, each work order having value of Rs. 7 Cr.</li></ul> |

| Sr. | RFP Clause / Section               | Existing Clause (As Issued)                                                                                                                                                                                                        | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 75  | 2. Eligibility Criteria; page no 8 | Attachments:<br>Details of such projects undertaken along with work order/purchase order copy/client's on-going (along with client certificate)/ completion certification with the details w.r.t to the clause should be enclosed. | <p>We humbly request the Purchaser to kindly clarify and modify the clause to explicitly allow submission of a Chartered Accountant (CA) Certificate, duly supported by relevant supporting documents, as acceptable evidence for demonstrating project experience and project value.</p> <p>Accordingly, the clause may be revised as follows:</p> <p>"Details of such projects undertaken along with Work Order/Purchase Order copy and any one of the following supporting documents: Client Completion Certificate, Client On-going Project Certificate, CA Certificate certifying the project value and scope duly supported by Work Orders/Agreements/Invoices, or any other documentary evidence establishing compliance with the eligibility criteria."</p> <p>This amendment will ensure fair participation by experienced bidders who have successfully executed similar projects but may not be able to obtain completion or ongoing project certificates from customers due to organizational policies, project confidentiality obligations, administrative constraints, security, SOC, data centre, cloud, or ICT infrastructure proje</p>                                                                                                                                                                                                                                                                                                                                                                                                    | <p>For Eligibility criteria, page no 8, Sr. no.2 &amp; 3 attachment(s) revised to:</p> <p>The copies of Audited Annual Accounts/Balance Sheet along with Profit &amp; Loss Account and CA Certified Statement for last three financial years as on bid submission shall be attached along with the bid. UDIN number should available in CA certificate. for FY25-26, if audited BS and P&amp;L is not available, bidder may submit CA certfid unaudited BS and PL along with clearly visible UDIN number.</p> |
| 76  | RFP Clause - 8.4; page no 29       | HLD/LLD and hardware delivery within 2-4 weeks from PO.                                                                                                                                                                            | <p>The proposed solution involves supply of specialized ICT and Cybersecurity infrastructure, comprising multiple OEM products, hardware appliances, software licenses, and associated components that are often sourced through global supply chains. While the bidder can complete the solution design activities, architecture finalization, and submission of HLD/LLD within the stipulated 2-4 weeks, the procurement and delivery of hardware is dependent upon OEM manufacturing schedules, order processing, logistics arrangements, customs clearance (where applicable), and transportation lead times.</p> <p>In the current market environment, several critical infrastructure components continue to experience extended procurement cycles owing to global supply chain constraints, semiconductor availability, import dependencies, and increased demand for enterprise-grade hardware. Consequently, a hardware delivery timeline of 12-14 weeks is more practical and aligned with prevailing industry standards for infrastructure projects of similar size and complexity.</p> <p>The requested extension will enable the successful bidder to procure genuine OEM equipment, ensure compliance with all technical specifications, conduct proper quality checks, and deliver the complete infrastructure without compromising solution quality or project objectives. The proposed modification will not impact the overall planning and design activities, as the HLD/LLD timelines are being retained as originally specified.</p> | See corrigendum point 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Sr. | RFP Clause / Section          | Existing Clause (As Issued)                                                                  | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Responses  |
|-----|-------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|     |                               |                                                                                              | Accordingly, we request the Purchaser to kindly amend the hardware delivery timeline to 12-14 weeks from the date of PO, while retaining the HLD/LLD submission timeline of 2-4 weeks, thereby ensuring realistic project execution timelines and wider participation of qualified bidders.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |
| 77  | RFP Clause 7.1; page no 25-26 | Quarterly penalties capped at 25% of quarterly charges; project penalties capped separately. | <p>The purpose of SLA credits and penalties is to incentivize service performance and contractual compliance rather than create an unlimited financial exposure for the successful bidder. Uncapped and overlapping penalty provisions may lead to disproportionate commercial risk and uncertainty, which can adversely impact project pricing and bidder participation.</p> <p>Further, a cap of 10% of Quarterly O&amp;M Charges for SLA-related deductions is a reasonable and widely accepted industry practice for long-term IT, cybersecurity, cloud, and managed service engagements. Similar provisions are commonly adopted in public-sector procurements to ensure that service deductions remain proportionate to the value of services being delivered. For example, some RFPs cap total quarterly O&amp;M penalties at 10% of the due quarterly payment.</p> <p>In addition, capping the overall LD/penalty exposure at 10% of the Total Contract Value provides a balanced risk allocation between the Purchaser and the successful bidder and is aligned with prevailing market practices for large technology projects. Comparable tender documents have also adopted overall project penalty caps to ensure that remedies remain reasonable and commercially sustainable.</p> <p>The requested clarification regarding no double recovery is equally important, as a single incident may otherwise trigger multiple deductions under different SLA, LD, and penalty provisions. Applying multiple recoveries for the same event would result in duplicate financial impact without providing any additional contractual benefit. Industry practice generally provides that where multiple breaches arise from the same root cause, only one deduction or the highest applicable deduction should be considered.</p> <p>Accordingly, we request the Purchaser to kindly confirm the above caps and the principle of no double recovery to ensure equitable risk allocation, encourage wider participation from competent bidders, and maintain the long-term financial viability of the engagement.</p> | As per RFP |

| Sr. | RFP Clause / Section                                                                                    | Existing Clause (As Issued)                                                                                                                                          | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Responses                                                                                                                                                                                                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 78  | Section 5.1 "Technical Specification". Requirement "SSL/TLS Connection Per Session" / Sr.-3; Page no 16 | Minimum 100 KCPS                                                                                                                                                     | Prebid Query / Justification - Selective decryption is having Lower performance overhead: Processing capacity is reserved for high-risk or protected traffic instead of decrypting every TLS session.<br>Higher mitigation throughput: The appliance can handle more concurrent connections and attack traffic.<br><br>Change request : We request to change clause as "DDoS mitigation solution should support minimum 100 K SSL CPS with selective decrvption using TLS proxy"          | Section 5.1 Sr. 7 revised: DDoS mitigation solution should support minimum 100 KCPS with decryption using TLS proxy or Hardware TLS acceleration                                                                                                                                                                       |
| 79  | Section 5.2.3. "Technical Specification". SSL/TLS Decryption for DDoS / Sr-2; Page no 18                | SSL/TLS Decryption for DDoS. "Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"      | Prebid Query / Justification: Modern DDoS mitigation solution use TLS proxy for TLS 1.3 PFS decryption using TLS fingerprinting and selective decryption. Selective decryption helps in achieving higher performance.<br><br>Change request : We request to change clause as "Hardware-accelerated or Proxy based TLS 1.2 ECDHE and TLS 1.3 PFS decryption for application-layer inspection; TLS inspection throughput Minimum 100 K CPS using selective decryption / TLS fingerprinting" | Section 5.2.3. Sr, 2 revised: SSL/TLS Decryption for DDoS. "Hardware-accelerated or TLS proxy based TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                                                                       |
| 80  | Section 5.2.3. "Technical Specification". API Protection / Sr-5; Page no 18                             | Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection                                                                                                | Prebid Query / Justification: Asked feature will make DDoS mitigation solution stateful and prone to state exhaustion attacks.<br><br>Change request : We request to change point as "System should have capability for source rate limit on URI or REGEX of URI"                                                                                                                                                                                                                         | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                 |
| 81  | Section 5.3. "Technical Specification". Signature-Based Detection / Sr-3; Page no 19                    | Pre-built library of DDoS attack signatures; real-time signature updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. | Change request : We request to change clause as "Pre-built library of DDoS attack signatures / reputation feed; real-time signature / reputation feeds updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. System should have support up to 10 Million IoC's and should integrate on STIX / TAXI with third party Threat Intelligence Platform "                                                                                          | Section 5.3. Sr. 3 revised: Pre-built library of DDoS attack signatures/reputation feed; real-time signature/reputation feed updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. Preferably support integration with Third party intelligence using STIX/TAXI for IOCs |
| 82  | Section 5.3. "Technical Specification". False Positive Rate / Sr-3; Page no 19                          | Bidder to demonstrate false positive rate of < 1% in reference deployment.                                                                                           | Prebid Query / Justification": Asked feature need more clarity in terms of false positive generation on DDoS mitigation engine along with classification of False Positive rate.                                                                                                                                                                                                                                                                                                          | Clause Removed                                                                                                                                                                                                                                                                                                         |
| 83  | Section 5.6. "Technical Specification". Reporting Requirement / Sr-4; Page no 22                        | Reports suitable for regulatory audit: ISO 27001, Cybersecurity framework compliance posture.                                                                        | Change request : We request to change clause as "Reports suitable for regulatory audit: as per Cybersecurity framework compliance posture."                                                                                                                                                                                                                                                                                                                                               | Section 5.6. Sr. 4 revised: Reports suitable for regulatory audit and Cybersecurity framework compliance posture.                                                                                                                                                                                                      |
| 84  | Section 7.1 Appliance Uptime & Availability; Sr-10; Page no 26                                          | Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 7 working days                                                                                    | Justification: Hotfix/patch/vulnerability deployment depends on severity of issue.<br><br>Change request: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 15 working days or any work around.                                                                                                                                                                                                                                                                          | 7.1 Appliance Uptime & Availability Sr10 clause revised: Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 14 days                                                                                                                                                                                    |

| Sr. | RFP Clause / Section                                                         | Existing Clause (As Issued)                                                                                                                                                                                                                                                                                                | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 85  | Section 4.2.5 Implementation/ Operation; Page no23                           | OEM/ISV to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc.     | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "OEM/ISV/Bidder to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM/ISV/Bidder every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc." | Section 4.2.5 clause revised: OEM/Top tier OEM authorized Partner to assess and certify the implementation, hardening and configuration of the solution. Onsite Health check should be carried out by OEM/Top tier OEM authorized Partner every haft -year and yearly complete assessment to ensure the quality of implementation and operations by OEM/Top tier OEM authorized Partner itself of CPU utilization, database activities, OS status, etc. |
| 86  | Section 4.2.5 Implementation/ Operation; Page no 23                          | The OEM shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue. | Justification: As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><br>Change request: "The OEM/Bidder shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/Bidder/tenderer's team suitable rectification steps/proper Support shall be provided till eradication of the issue." | Section 4.2.5 clause revised: The bidder's team shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/bidder's team suitable rectification steps/proper Support shall be provided by OEM till eradication of the issue.                                                                                 |
| 87  | 8.4 Delivery & Implementation Timeline / Payment Schedule; Sr - 4; Page no30 | 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: in 20 equal instalments at the end of every Quarter.                                                                                                                                                                                             | Justification: We request to change this clause as follows:<br><br>Change request: 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: Yearly advance                                                                                                                                                                                                                                                                                                                                          | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 88  | Page no 17                                                                   | Physical hardware specification-- Specifically mandate 16*10 GB Bypass ports SR or LR fiber ports                                                                                                                                                                                                                          | Please clarify how many SR Ports and LR ports require from day one, As we understand from the RFP there are only two ISP links provisioned for which Four ports On-prem DDoS are sufficient and for future expansion of Four more ISP links, we will need 8 more ports on on prem hardware. Hence we request to reduce 16 ports to 12 ports.                                                                                                                                                                         | Section 5.1Revised clause: 10. Specifically mandates 16 x 10 GigE bypass ports (SR) fiber ports, and hot- swappable dual power supplies                                                                                                                                                                                                                                                                                                                 |
| 89  | Page no 16                                                                   | Throughput License capacity -- 100 Gbps                                                                                                                                                                                                                                                                                    | We request to amend as mentioned below:<br>100 Gbps clean guaranteed traffic and 200 Gbps of inspection traffic                                                                                                                                                                                                                                                                                                                                                                                                      | Section 5.1 Sr. 3 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load.                                                                                                                                                                                          |

| Sr. | RFP Clause / Section | Existing Clause (As Issued)                                                                                                                                                                                    | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 90  | Page no 16           | Inspection Throughput -- 100 Gbps bidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load.                                          | As Industry standard ISP links are burstable in nature and under those circumstances the proposed solution must be scalable.<br>We request to amend as mentioned below:<br>Inspection Throughput -- 100 Gbps unidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load. | Section 5.1 Sr. 4 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load.                                                                                                                                                                           |
| 91  | Page no 22           | MTBF of Appliance -- Minimum 100000 hours MTBF for hardware chassis.                                                                                                                                           | We request to amend as mentioned below:<br>Reduce from 100000 to 80000 Hours MTBF.                                                                                                                                                                                                                                                                | Revised Clause 6 of 5.7 MTBF of Appliance: Minimum 70,000 hours MTBF or more for the hardware chassis<br>Revised Clause 6 Technical Compliance Checklist E6: MTBF ≥ 70,000 hours                                                                                                                                                                                                                                                         |
| 92  | Page no 19           | Real Time Attack Detection -- Detection to mitigation time : maximum 18 seconds for automated signature activation; desirable < 10 Seconds                                                                     | Solution should support mitigation of Burst Attacks in zero-time by an automatically created signature within 12 secs and must be mentioned on data sheet; and desirable < 10 Seconds                                                                                                                                                             | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                                                                                                                                   |
| 93  | Page no 9            | OEM should have supplied an Anti-DDoS solution having value of ₹50 Cr. Work order should be available in the last three financial years as on bid submission.                                                  | Amend as mentioned below: OEM should have supplied an Anti-DDoS solution having value of 30 Cr. Work order should be available in the last three financial years as on bid submission.                                                                                                                                                            | 2. Eligibility Criteria Sr 4 revised: OEM Should have supplied Anti-DDoS solution having value of Rs. 30 cr. work order should be available in the last three financial years as on bid submission.                                                                                                                                                                                                                                      |
| 94  | Page no 8-9          | Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr. | Amend as mentioned below: Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS Solution/ Cyber security solutions in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr.                                                                                | 2. Eligibility Criteria point 4. clause revised: The bidder should have experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution / Anti-DDoS solution as a part of cyber security solution in last three financial years.<br>• One work order having value of Rs. 13 Cr or<br>• Two work order, each work order having value of Rs. 10 Cr or<br>• Three work order, each work order having value of Rs. 7 Cr. |
| 95  | Page no 17           | Behavior rate limiting fingerprinting, CAPTCHA challenge, rate limiting per source IP                                                                                                                          | We request to amend as mentioned below: Behavior Rate limiting/Captcha Challenge/rate limiting per source IP address                                                                                                                                                                                                                              | Section 5.2.2 Sr 2 revised: HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, rate limiting per source IP                                                                                                                                                                                                                                                                                                                     |
| 96  | Page no 17           | Rate limiting on REST/SOAP API endpoints JSON/XML payload inspection                                                                                                                                           | We request to remove as this compliance point is specific to application and app sec security.                                                                                                                                                                                                                                                    | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                                                                                                                                   |
| 97  |                      | TLS 1.3 Perfect Forward Secrecy (PFS) HW Acceleration Support and Dynamic TLS Fingerprint                                                                                                                      | TLS 1.3 PFS Hardware Acceleration ensures high-speed inspection of encrypted traffic without performance impact, while Dynamic TLS Fingerprinting enables accurate identification and mitigation of malicious bots and encrypted Layer 7 attacks                                                                                                  | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 98  |                      | The solution must support TLS traffic inspection in asymmetric deployments, without requiring visibility of both inbound and outbound flows                                                                    | For enabling effective detection and mitigation of encrypted threats in asymmetric network architectures where only one traffic direction is visible, eliminating the need for full bidirectional flow visibility.                                                                                                                                | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Sr. | RFP Clause / Section | Existing Clause (As Issued)                                                                                                                                           | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                      |
|-----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 99  |                      | Zero day Burst attack protection                                                                                                                                      | Zero-day burst attack protection is essential to detect and mitigate previously unknown, rapidly emerging attack patterns in real time before signatures or manual countermeasures become available.                                                                                                                                              | As per RFP                                                                                                                                                                                                                                                     |
| 100 |                      | Offered platform lineup powered by FPGA hardware acceleration with higher maximum performance throughput and packets per second (PPS) consistently.                   | It always best practice to consider FPGA hardware acceleration delivers consistently high throughput and PPS performance, ensuring real-time attack mitigation with low latency and predictable performance even during large-scale DDoS attacks.                                                                                                 | As per RFP                                                                                                                                                                                                                                                     |
| 101 |                      | Support IP Mode - Solution includes the option to detect and mitigate in transparent mode (L2) and at the IP level (L3)                                               | Support for both L2 transparent and L3 IP deployment modes provides flexibility to integrate the DDoS solution into diverse network architectures with minimal disruption and optimal traffic visibility.                                                                                                                                         | As per RFP                                                                                                                                                                                                                                                     |
| 102 |                      | Automatic generated reports and analysis separately for every attack life cycle * Real time automatic attack remediation and attack prevention (AI based)             | Automatic attack lifecycle reporting and AI-based real-time remediation provide immediate threat visibility, faster response, and proactive mitigation of evolving attacks with minimal manual intervention                                                                                                                                       | As per RFP                                                                                                                                                                                                                                                     |
| 103 | Page no 17           | Physical hardware specification-- Specifically mandate 16*10 GB Bypass ports SR or LR fiber ports                                                                     | Please clarify how many SR Ports and LR ports require from day one, As we understand from the RFP there are only two ISP links provisioned for which Four ports On-prem DDoS are sufficient and for future expansion of Four more ISP links, we will need 8 more ports on on prem hardware. Hence we request to reduce 16 ports to 12 ports.      | Section 5.1 Revised clause: 10. Specifically mandates 16 x 10 GigE bypass ports (SR) fiber ports, and hot- swappable dual power supplies                                                                                                                       |
| 104 | Page no 16           | Throughput License capacity -- 100 Gbps                                                                                                                               | We request to amend as mentioned below:<br>100 Gbps clean guaranteed traffic and 200 Gbps of inspection traffic                                                                                                                                                                                                                                   | Section 5.1 Sr. 3 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load. |
| 105 | Page no 16           | Inspection Throughput -- 100 Gbps bidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load. | As Industry standard ISP links are burstable in nature and under those circumstances the proposed solution must be scalable.<br>We request to amend as mentioned below:<br>Inspection Throughput -- 100 Gbps unidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load. | Section 5.1 Sr. 4 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load. |
| 106 | Page no 22           | MTBF of Appliance -- Minimum 100000 hours MTBF for hardware chassis.                                                                                                  | We request to amend as mentioned below:<br>Reduce from 100000 to 80000 Hours MTBF.                                                                                                                                                                                                                                                                | Revised Clause 6 of 5.7 MTBF of Appliance: Minimum 70,000 hours MTBF or more for the hardware chassis<br>Revised Clause 6 Technical Compliance Checklist E6: MTBF ≥ 70,000 hours                                                                               |

| Sr. | RFP Clause / Section | Existing Clause (As Issued)                                                                                                                                                                                    | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                  | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 107 | Page no 19           | Real Time Attack Detection --<br>Detection to mitigation time : maximum 18 seconds for automated signature activation; desirable < 10 Seconds                                                                  | Solution should support mitigation of Burst Attacks in zero-time by an automatically created signature within 12 secs and must be mentioned on data sheet; and desirable < 10 Seconds                                                                                                                                                         | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                                                                                                                                   |
| 108 | Page no 9            | OEM should have supplied an Anti-DDoS solution having value of ₹50 Cr. Work order should be available in the last three financial years as on bid submission.                                                  | Amend as mentioned below: OEM should have supplied an Anti-DDoS solution having value of 30 Cr. Work order should be available in the last three financial years as on bid submission.                                                                                                                                                        | 2. Eligibility Criteria Sr 4 revised: OEM Should have supplied Anti-DDoS solution having value of Rs. 30 cr. work order should be available in the last three financial years as on bid submission.                                                                                                                                                                                                                                      |
| 109 | Page no 8-9          | Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr. | Amend as mentioned below: Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS Solution/ Cyber security solutions in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr.                                                                            | 2. Eligibility Criteria point 4. clause revised: The bidder should have experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution / Anti-DDoS solution as a part of cyber security solution in last three financial years.<br>• One work order having value of Rs. 13 Cr or<br>• Two work order, each work order having value of Rs. 10 Cr or<br>• Three work order, each work order having value of Rs. 7 Cr. |
| 110 | Page no 17           | Behavior rate limiting fingerprinting, CAPTCHA challenge, rate limiting per source IP                                                                                                                          | We request to amend as mentioned below: Behavior Rate limiting/Captcha Challenge/rate limiting per source IP address                                                                                                                                                                                                                          | Section 5.2.2 Sr 2 revised: HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, rate limiting per source IP                                                                                                                                                                                                                                                                                                                     |
| 111 | Page no 17           | Rate limiting on REST/SOAP API endpoints JSON/XML payload inspection                                                                                                                                           | We request to remove as this compliance point is specific to application and app sec security.                                                                                                                                                                                                                                                | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                                                                                                                                   |
| 112 |                      | TLS 1.3 Perfect Forward Secrecy (PFS) HW Acceleration Support and Dynamic TLS Fingerprint                                                                                                                      | TLS 1.3 PFS Hardware Acceleration ensures high-speed inspection of encrypted traffic without performance impact, while Dynamic TLS Fingerprinting enables accurate identification and mitigation of malicious bots and encrypted Layer 7 attacks                                                                                              | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 113 |                      | The solution must support TLS traffic inspection in asymmetric deployments, without requiring visibility of both inbound and outbound flows                                                                    | For enabling effective detection and mitigation of encrypted threats in asymmetric network architectures where only one traffic direction is visible, eliminating the need for full bidirectional flow visibility.                                                                                                                            | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 114 |                      | Zero day Burst attack protection                                                                                                                                                                               | Zero-day burst attack protection is essential to detect and mitigate previously unknown, rapidly emerging attack patterns in real time before signatures or manual countermeasures become available.                                                                                                                                          | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 115 |                      | Offered platform lineup powered by FPGA hardware acceleration with higher maximum performance throughput and packets per second (PPS) consistently.                                                            | It always best practice to consider FPGA hardware acceleration delivers consistently high throughput and PPS performance, ensuring real-time attack mitigation with low latency and predictable performance even during large-scale DDoS attacks.                                                                                             | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 116 |                      | Support IP Mode - Solution includes the option to detect and mitigate in transparent mode (L2) and at the IP level (L3)                                                                                        | Support for both L2 transparent and L3 IP deployment modes provides flexibility to integrate the DDoS solution into diverse network architectures with minimal disruption and optimal traffic visibility.                                                                                                                                     | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 117 |                      | Automatic generated reports and analysis separately for every attack life cycle * Real time automatic attack remediation and attack prevention (AI based)                                                      | Automatic attack lifecycle reporting and AI-based real-time remediation provide immediate threat visibility, faster response, and proactive mitigation of evolving attacks with minimal manual intervention                                                                                                                                   | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 118 | Page no 17           | Physical hardware specification-- Specifically mandate 16*10 GB Bypass ports SR or LR fiber ports                                                                                                              | Please clarify how many SR Ports and LR ports require from day one, As we understand from the RFP there are only two ISP links provisioned for which Four ports On-prem Dodos are sufficient and for future expansion of Four more ISP links, we will need 8 more ports on on prem hardware. Hence we request to reduce 16 ports to 12 ports. | Section 5.1 Revised clause: 10. Specifically mandates 16 x 10 GigE bypass ports (SR) fiber ports, and hot- swappable dual power supplies                                                                                                                                                                                                                                                                                                 |

| Sr. | RFP Clause / Section | Existing Clause (As Issued)                                                                                                                                                                                    | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                      | Responses                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 119 | Page no 16           | Throughput License capacity -- 100 Gbps                                                                                                                                                                        | We request to amend as mentioned below:<br>100 Gbps clean guaranteed traffic and 200 Gbps of inspection traffic                                                                                                                                                                                                                                   | Section 5.1 Sr. 3 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load.                                                                                                                                                                           |
| 120 | Page no 16           | Inspection Throughput -- 100 Gbps bidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load.                                          | As Industry standard ISP links are burstable in nature and under those circumstances the proposed solution must be scalable.<br>We request to amend as mentioned below:<br>Inspection Throughput -- 100 Gbps unidirectional inspection AND mitigation throughput(not inspection-only). Throughput must be guaranteed under full DDoS attack load. | Section 5.1 Sr. 4 revised: The proposed solution must guarantee 100 Gbps bidirectional inspection and mitigation throughput — not inspection-only — sustained under full-volume DDoS attack conditions, including combined attack and legitimate traffic load.                                                                                                                                                                           |
| 121 | Page no 22           | MTBF of Appliance -- Minimum 100000 hours MTBF for hardware chassis.                                                                                                                                           | We request to amend as mentioned below:<br>Reduce from 100000 to 80000 Hours MTBF.                                                                                                                                                                                                                                                                | Revised Clause 6 of 5.7 MTBF of Appliance: Minimum 70,000 hours MTBF or more for the hardware chassis<br>Revised Clause 6 Technical Compliance Checklist E6: MTBF ≥ 70,000 hours                                                                                                                                                                                                                                                         |
| 122 | Page no 19           | Real Time Attack Detection -- Detection to mitigation time : maximum 18 seconds for automated signature activation; desirable < 10 Seconds                                                                     | Solution should support mitigation of Burst Attacks in zero-time by an automatically created signature within 12 secs and must be mentioned on data sheet; and desirable < 10 Seconds                                                                                                                                                             | Section 5.3, Sr.2 revised: Detection-to-mitigation time: maximum 18 seconds for automated signature/counter measure activation; desirable ≤ 10 seconds                                                                                                                                                                                                                                                                                   |
| 123 | Page no 9            | OEM should have supplied an Anti-DDoS solution having value of ₹50 Cr. Work order should be available in the last three financial years as on bid submission.                                                  | Amend as mentioned below: OEM should have supplied an Anti-DDoS solution having value of 30 Cr. Work order should be available in the last three financial years as on bid submission.                                                                                                                                                            | 2. Eligibility Criteria Sr 4 revised: OEM Should have supplied Anti-DDoS solution having value of Rs. 30 cr. work order should be available in the last three financial years as on bid submission.                                                                                                                                                                                                                                      |
| 124 | Page no 8-9          | Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr. | Amend as mentioned below: Experience in Supply, Installation, Testing and Commissioning of Anti-DDoS Solution/ Cyber security solutions in last three financial years. ANY ONE: 1 work order ≥₹16 Cr OR 2 work orders, each ≥₹10 Cr OR 3 work orders, each ≥₹8 Cr.                                                                                | 2. Eligibility Criteria point 4. clause revised: The bidder should have experience in Supply, Installation, Testing and Commissioning of Anti-DDoS solution / Anti-DDoS solution as a part of cyber security solution in last three financial years.<br>• One work order having value of Rs. 13 Cr or<br>• Two work order, each work order having value of Rs. 10 Cr or<br>• Three work order, each work order having value of Rs. 7 Cr. |
| 125 | Page no 17           | Behavior rate limiting fingerprinting, CAPTCHA challenge, rate limiting per source IP                                                                                                                          | We request to amend as mentioned below: Behavior Rate limiting/Captcha Challenge/rate limiting per source IP address                                                                                                                                                                                                                              | Section 5.2.2 Sr 2 revised: HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, rate limiting per source IP                                                                                                                                                                                                                                                                                                                     |
| 126 | Page no 17           | Rate limiting on REST/SOAP API endpoints JSON/XML payload inspection                                                                                                                                           | We request to remove as this compliance point is specific to application and app sec security.                                                                                                                                                                                                                                                    | Section 5.2.3. "Technical Specification". (Sr 5) API Protection Revised clause revised to "System should have capability for source rate limit on URI or REGEX of URI" Additionally refer section 5.1 clause 6 of RFP.                                                                                                                                                                                                                   |
| 127 |                      | TLS 1.3 Perfect Forward Secrecy (PFS) HW Acceleration Support and Dynamic TLS Fingerprint                                                                                                                      | TLS 1.3 PFS Hardware Acceleration ensures high-speed inspection of encrypted traffic without performance impact, while Dynamic TLS Fingerprinting enables accurate identification and mitigation of malicious bots and encrypted Layer 7 attacks                                                                                                  | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 128 |                      | The solution must support TLS traffic inspection in asymmetric deployments, without requiring visibility of both inbound and outbound flows                                                                    | For enabling effective detection and mitigation of encrypted threats in asymmetric network architectures where only one traffic direction is visible, eliminating the need for full bidirectional flow visibility.                                                                                                                                | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 129 |                      | Zero day Burst attack protection                                                                                                                                                                               | Zero-day burst attack protection is essential to detect and mitigate previously unknown, rapidly emerging attack patterns in real time before signatures or manual countermeasures become available.                                                                                                                                              | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Sr. | RFP Clause / Section | Existing Clause (As Issued)                                                                                                                               | Query / Clarification Sought                                                                                                                                                                                                                      | Responses                             |
|-----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 130 |                      | Offered platform lineup powered by FPGA hardware acceleration with higher maximum performance throughput and packets per second (PPS) consistently.       | It always best practice to consider FPGA hardware acceleration delivers consistently high throughput and PPS performance, ensuring real-time attack mitigation with low latency and predictable performance even during large-scale DDoS attacks. | As per RFP                            |
| 131 |                      | Support IP Mode - Solution includes the option to detect and mitigate in transparent mode (L2) and at the IP level (L3)                                   | Support for both L2 transparent and L3 IP deployment modes provides flexibility to integrate the DDoS solution into diverse network architectures with minimal disruption and optimal traffic visibility.                                         | As per RFP                            |
| 132 |                      | Automatic generated reports and analysis separately for every attack life cycle * Real time automatic attack remediation and attack prevention (AI based) | Automatic attack lifecycle reporting and AI-based real-time remediation provide immediate threat visibility, faster response, and proactive mitigation of evolving attacks with minimal manual intervention                                       | May be provided as additional feature |

Apart from the above pre-bid queries and the corrigendum, all other terms and conditions of the RFP shall remain unchanged.