

| Corrigendum - 2                                                                                                                                                                                                                                                                          |                                                                                                              |                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 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) |                                                                                                              |                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                        |
| Sr                                                                                                                                                                                                                                                                                       | RFP Clause / Section                                                                                         | Existing Clause (As Issued)                                                                                                                                                             | Query / Clarification Sought                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Responses                                                              |
| 1                                                                                                                                                                                                                                                                                        | 4.1 Broad Scope (Page-11)                                                                                    | Supply of Anti-DDoS hardware appliances with all necessary accessories, rack units, transceivers, and inter-connect cables                                                              | Kindly confirm that Bidder should provide the RACK Units also, Or existing RACK can be utilised                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | As per RFP                                                             |
| 2                                                                                                                                                                                                                                                                                        | 4.1 Broad Scope (Page-11)                                                                                    | Integration with SDC's existing network infrastructure: upstream routers, core switches, firewalls, load balancers                                                                      | Kindly confirm the<br>a) Current Router Make & Model,<br>b) Are the link terminated on Copper or Fiber<br>d) Bandwidth of each links                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | if require bidder may conduct site visit to understand existing infra. |
| 3                                                                                                                                                                                                                                                                                        | 4.1 Broad Scope (Page-11)                                                                                    | BGP peering configuration with SDC's two (02) upstream ISPs for traffic diversion during volumetric attacks                                                                             | a) Number of Internet Links & Provider<br>b) With appliance based DDOS does the bidder need to provide Volumetric DDOS solution bundled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | as per corrigendum 1                                                   |
| 4                                                                                                                                                                                                                                                                                        | 4.2.1 Hardware Supply and Deployment                                                                         | Cabling, labeling, and physical installation as per SDC standards                                                                                                                       | Will SDC Provide the Cabling or Bidder need to consider the cabling for provided hardware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | As per RFP                                                             |
| 5                                                                                                                                                                                                                                                                                        | 4.2.2 Network Integration                                                                                    | IP prefix advertisement and withdrawal automation during attack onset and clearance                                                                                                     | Current number of IP Prefix with both Internet links                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | two /24 ip subnet, may increase in future                              |
| 6                                                                                                                                                                                                                                                                                        | 4.2.1 Hardware Supply and Deployment                                                                         | Supply, rack, and stack of DDOS appliances in GoG's State data centers                                                                                                                  | Kindly confirm its only GoG is only one DC or there are multi location DC-DR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | only DC location                                                       |
| 7                                                                                                                                                                                                                                                                                        |                                                                                                              | Limitation of Liability of the Bidder                                                                                                                                                   | The total aggregate liability of the bidder shall be limited to 12 months of the charges received from the customer under a specific purchase order, giving rise to the claims. Neither of the parties shall be liable for any Indirect and consequential damages under the RFP.                                                                                                                                                                                                                                                                                                                                                                         | As per RFP                                                             |
| 8                                                                                                                                                                                                                                                                                        | Additional Clause                                                                                            | Subsidiary/Affiliate                                                                                                                                                                    | Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary. Please confirm Also, please allow the bidder to use the documents from parent company for qualification on Eligibility, experience, references, etc.                                                                                                                                                                                                                                              | As per RFP                                                             |
| 9                                                                                                                                                                                                                                                                                        | Facility Management Support (FMS)                                                                            | Dedicated onsite FMS engineer at DC during business hours (10:00 – 19:00 hrs) on working days, In case of leave/absence replacement must be provided with prior intimation.             | Do you required 1 On-site engineer during bussiness Hours, or Should we consider 24/7/365 for On-site support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per RFP                                                             |
| 10                                                                                                                                                                                                                                                                                       | Facility Management Support (FMS)                                                                            | Dedicated onsite FMS engineer at DC during business hours (10:00 – 19:00 hrs) on working days, In case of leave/absence replacement must be provided with prior intimation.             | What is the Businnes hours Mon-Friday or Mon-Sunday                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | As per RFP                                                             |
| 11                                                                                                                                                                                                                                                                                       | Facility Management Support (FMS)                                                                            | onsite FMS engineer have to present within 1 hour as and when required (beyond regular timing), This timing is indicative liable to vary as and when required without prior intimation. | Instead on-site FMS engineer required in 1 hrs can be consider immediate remote support after bussiness hours, & arrange on-site support on best feasibility                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                             |
| 12                                                                                                                                                                                                                                                                                       | <b>Section 5.1</b> "Technical Specification". Requirement "Hardware Architecture" / <b>(Sr-1 / Page# 16)</b> | Purpose-built DDOS mitigation appliance; NOT a general-purpose x86 COTS server repurposed for DDOS. Must have dedicated ASIC / NPU / FPGA for packet processing.                        | <b>Prebid Query / Justification :</b> 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><b>Change request :</b> We request to remove this point and change cluase as " <b>Purpose-built DDOS mitigation appliance; NOT a general-purpose platform and should not be part of any UTM or Load Balancer</b> " | As per Corrigendum 1                                                   |

|    |                                                                                                                     |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                      |
|----|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | Section 5.1 "Technical Specification". Requirement "External Intelligent Bypass / Fail-open" /<br>(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. | <b>Prebid Query / Justification</b> : 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><b>Change request</b> : 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. | As per Corrigendum 1                                                                                                                                                 |
| 14 | Section 5.1 "Technical Specification". Requirement "SSL/TLS Connection Per Session" /<br>(Sr-3 / Page# 16)          | Minimum 100 KCPS                                                                                                                                                                                                     | <b>Prebid Query / Justification - Selective decryption is having Lower performance overhead</b> : Processing capacity is reserved for high risk or protected traffic instead of decrypting every TLS session.<br><b>Higher mitigation throughput</b> : The appliance can handle more concurrent connections and attack traffic.<br><br><b>Change request</b> : We request to change clause as "DDoS mitigation solution should support minimum 100 K SSL CPS with selective decryption using TLS proxy"                                                                                                                       | As per Corrigendum 1                                                                                                                                                 |
| 15 | Section 5.1 "Technical Specification". Requirement "Network Interfaces" /<br>(Sr-11 / Page# 17)                     | Minimum 16 x 10GE/25GE SFP28 ports for management and monitoring.                                                                                                                                                    | <b>Prebid Query / Justification</b> : We do not need more than two out of band ports for management and monitoring.<br><b>Change request</b> : 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 1GE or 2 x 10GE copper out of band management ports. |
| 16 | Section 5.2.2 "Technical Specification". Requirement "Protocol Attacks" /<br>(Sr-2 / Page# 18)                      | Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioural fingerprinting, CAPTCHA challenge, rate limiting per source IP"                                                      | <b>Prebid Query / Justification</b> : CAPTCHA Challenge is older authentication method and is intrusive, also will make DDoS mitigation solution stateful.<br><br><b>Change request</b> : We request to remove CAPTCHA and change clause as "Attack Vector "HTTP/HTTPS GET / POST" Flood (L7)<br>Minimum Mitigation Requirement "Behavioural fingerprinting, rate limiting per source IP"                                                                                                                                                                                                                                     | As per Corrigendum 1                                                                                                                                                 |
| 17 | Section 5.2.2 "Technical Specification". Requirement "Protocol Attacks" /<br>(Sr-6 / Page# 18)                      | Hardware TLS acceleration for inspection; TLS handshake rate limiting                                                                                                                                                | <b>Prebid Query / Justification</b> : 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><b>Change request</b> : We request to change clause as "Hardware TLS acceleration or Proxy based TLS inspection; TLS handshake rate limiting"                                                                                                                                                                                                                                            | As per Corrigendum 1                                                                                                                                                 |
| 18 | Section 5.2.3. "Technical Specification". SSL/TLS Decryption for DDoS /<br>(Sr-2 / Page# 18)                        | SSL/TLS Decryption for DDoS.<br>"Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS"                                                   | <b>Prebid Query / Justification</b> : 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><b>Change request</b> : 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"                                                                                                                      | As per Corrigendum 1                                                                                                                                                 |
| 19 | Section 5.2.3. "Technical Specification". API Protection /<br>(Sr-5 / Page# 18)                                     | Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection                                                                                                                                                | <b>Prebid Query / Justification</b> : Asked feature will make DDoS mitigation solution stateful and prone to state exhaustion attacks.<br><br><b>Change request</b> : We request to change point as "System should have capability for source rate limit on URI or REGEX of URI"                                                                                                                                                                                                                                                                                                                                              | As per Corrigendum 1                                                                                                                                                 |
| 20 | 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.                                                                                                         | <b>Change request</b> : We request to change clause as "Detection-to-mitigation time: maximum 18 seconds for automated signature / countermeasure activation; desirable ≤ 10 seconds."                                                                                                                                                                                                                                                                                                                                                                                                                                        | As per Corrigendum 1                                                                                                                                                 |
| 21 | 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.                                                  | <b>Change request</b> : 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 "                                                                                                                                                                                                                        | As per Corrigendum 1                                                                                                                                                 |

|    |                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 22 | <b>Section 5.3.</b> "Technical Specification". False Positive Rate /<br>( Sr-3 / Page# 19)                                                         | Bidder to demonstrate false positive rate of < 1% in reference deployment.                                                                                                                                                                                                                                                 | <b>Prebid Query / Justification":</b> Asked feature need more clarity in terms of false positive generation on DDoS mitigation engine along with classification of False Postivie rate.                                                                                                                                                                                                                                                                                                                                        | As per Corrigendum 1 |
| 23 | <b>Section 5.6.</b> "Technical Specification". Reporting Requirement /<br>( Sr-4 / Page# 22)                                                       | Reports suitable for regulatory audit: ISO 27001, cybersecurity framework compliance posture.                                                                                                                                                                                                                              | <b>Change request :</b> We request to change clause as " <b>Reports suitable for regulatory audit: as per cybersecurity framework compliance posture.</b> "                                                                                                                                                                                                                                                                                                                                                                    | As per Corrigendum 1 |
| 24 | <b>Section 7.1</b> Appliance Uptime & Availability<br>( Sr-10 / Page# 26)                                                                          | Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 7 working days                                                                                                                                                                                                                                          | <b>Justification:</b> Hotfix/patch/vulnerability deployment depends on severity of issue.<br><b>Change request:</b> Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 15 working days or any work around.                                                                                                                                                                                                                                                                                                     | As per Corrigendum 1 |
| 25 | <b>Section 4.2.5</b> 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.     | <b>Justification:</b> As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><b>Change request:</b> "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." | As per Corrigendum 1 |
| 26 | <b>Section 4.2.5</b> 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. | <b>Justification:</b> As an OEM-certified resource is being provided by the bidder to manage the operations, we request to change this clause as follows:<br><b>Change request:</b> "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." | As per Corrigendum 1 |
| 27 | <b>Section 8.4</b> Delivery & Implementation Timeline<br>( Sr-2 / Page# 29)                                                                        | Hardware delivery at DC: Within 2 - 4 weeks                                                                                                                                                                                                                                                                                | <b>Justification:</b> Globally the current lead time for hardware delivery is about 10 weeks, so we request to change this as follows.<br><b>Change request:</b> Hardware delivery at DC: Within 8 - 10 weeks                                                                                                                                                                                                                                                                                                                  | As per Corrigendum 1 |
| 28 | <b>2. Eligibility Criteria</b><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.                                                                                                                                                              | <b>Justification:</b> 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><b>Change request:</b> 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.                                                                                    | As per Corrigendum 1 |
| 29 | <b>8.4</b> 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.                                                                                                                                                                                             | <b>Justification:</b> We request to change this clause as follows:<br><b>Change request:</b> 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges: Yearly advance                                                                                                                                                                                                                                                                                                                                          | As per RFP           |
| 30 | <b>Section 5.4.</b> "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.                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | As per Corrigendum 1 |

|    |                                                                                                                                               |                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                      |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 31 | <b>Section 5.4.</b> "Technical Specification". Traffic Scrubbing & Mitigation Method. Surgical Mitigation /<br><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. | <b>Prebid Query / Justification:</b> 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><b>Change request :</b><br><br>We request to change spec as " <b>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. The signalling 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. No Data/information shall leave Indian Sub-continent at any point and shall adhere to MEITY, RBI and GOI Guidelines at all time during the contract period.</b> " | As per Corrigendum 1 |
| 32 | <b>Section 5.4.</b> "Technical Specification". Traffic Scrubbing & Mitigation Method. Blackholing / RTBH /<br><br>( Sr-4 / Page# 20)          | Remote Triggered Black Hole (RTBH) support via BGP for extreme volumetric events as last resort.                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per Corrigendum 1 |
| 33 | <b>Section 5.4.</b> "Technical Specification". Traffic Scrubbing & Mitigation Method. Rate Limiting /<br><br>( Sr-5 / Page# 20)               | Granular rate limiting: per source IP, per destination IP, per subnet, per protocol, per port — independently configurable.                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per Corrigendum 1 |
| 34 | <b>Section 5.4.</b> "Technical Specification". Traffic Scrubbing & Mitigation Method. Geo-based Filtering /<br><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 Corrigendum 1 |
| 35 | <b>Section 5.4.</b> "Technical Specification". Traffic Scrubbing & Mitigation Method. ACL / Blacklist / Whitelist /<br><br>( Sr-7 / Page# 20) | Dynamic and static ACL support: blacklist and whitelist IP ranges, autonomous systems (AS numbers), and CIDR blocks.                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per Corrigendum 1 |
| 36 | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | As per Corrigendum 1 |
| 37 | Page 29: 8.3 Performance Bank Guarantee (PBG)                                                                                                 | PBG: 10% of total contract value, valid for contract period + 6 months                                                                              | Bidder requests PBG amount to be reduced to 3% of total contract value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | As per RFP           |
| 38 | Page 11; 4.1 Broad Scope                                                                                                                      | 5-year comprehensive onsite warranty from Go-Live                                                                                                   | The 5 year OEM warranty will commence from date of delivery of Hardware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | As per RFP           |
| 39 | Page 30; Payment Schedule                                                                                                                     | As per table in RFP document                                                                                                                        | Bidder requests for below changes:<br>Capex-Cost of Anti DDoS solution including 5 Year Comprehensive warranty and OEM Support to be payable as below:<br>- 80% on Hardware, software, licenses delivery<br>- 10% on Installation<br>- 10% on Final Acceptance test<br>FMS Charges for Onsite resource to be payable in 20 equal instalments at the beginning of every Quarter.<br>Payments should be done in Net 30 days of invoicing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | As per RFP           |
| 40 | Page 30; PRICE BID SCHEDULE:                                                                                                                  | As per table in RFP document                                                                                                                        | Bidder requests for below changes:<br>Sr# 1 to include charges for Capex-Cost of Anti DDoS solution including 5 Year Comprehensive warranty and OEM Support<br>O&M cost should only include the FMS charges for onsite resource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | As per RFP           |
| 41 | Page 30; PRICE BID SCHEDULE                                                                                                                   | O&M cost should not be < 35% of total cost                                                                                                          | 5 Year Comprehensive warranty and OEM Support to be included in Sr# 1 (capex cost of solution).<br>O&M cost should only include the FMS charges for onsite resource. Condition for minimum 35% of total cost to be relaxed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | As per RFP           |

|    |                                                                                                                          |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 42 | Section 5.1 "Technical Specification". Requirement "DDoS Attack Flood Prevention Rate" /<br><br>( Sr-5 / Page# 16)       | Minimum 140 MPPS (Million Packet Per Second) for DDoS flood prevention rate                                                                                                                                                                                                                        | <p><b>Prebid Query / Justification :</b> Required throughput asked on H/w is 100 Gbps, keeping minimum routable packet on internet, packets which can be filled in 100 Gbps is roughly 175 MPPS. Keeping minimum packet size in consideration and packet per second attack in consideration we request to increase packet per second to 175 MPPS.</p> <p><b>Change request :</b> We request to remove this point and change clause as "Minimum 175 MPPS (Million Packet Per Second) for DDoS flood prevention rate"</p> <p><b>Justification :</b> Required throughput asked on H/w is 100 Gbps, keeping minimum routable packet on internet, packets which can be filled in 100 Gbps is roughly 175 MPPS. Keeping minimum packet size in consideration and packet per second attack in consideration we request to increase packet per second to 175 MPPS. So, we request to change this clause as below:</p> <p><b>Change request :</b> "Minimum 175 MPPS (Million Packet Per Second) for DDoS flood prevention rate"</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Section 5.1 Sr. 5 Revised: Minimum 150 MPPS (Million Packet Per Second) for DDoS flood prevention rate                                                                                                                                                                                                                                                                                                                             |
| 43 | Section 5.1 "Technical Specification". Requirement "External Intelligent Bypass / Fail-open" /<br><br>( 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.                                                                               | <p><b>Prebid Query / Justification :</b> 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.</p> <p><b>Change request :</b> 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.</p> <p><b>Justification :</b> The term "OEM approved" is broad and open to interpretation, which may result in bidders offering third-party bypass devices with varying levels of integration, testing, and support. Since the external hardware bypass is a critical component that directly impacts service availability and fail-open functionality during appliance failure scenarios, it is essential that the bypass solution be supplied and fully supported by the OEM of the proposed DDoS mitigation solution.</p> <p>Restricting the requirement to an OEM-supplied external hardware bypass solution ensures:</p> <ul style="list-style-type: none"> <li>- Single point of accountability for interoperability, support, and troubleshooting.</li> <li>- Consistent validation and qualification of the bypass mechanism with the offered DDoS platform.</li> <li>- Elimination of ambiguity regarding compatibility and long-term support commitments.</li> </ul> <p>Reduced operational and maintenance risks in production environments.</p> <p>Therefore, the words "or OEM approved" should be removed to ensure that only OEM-supplied and fully supported bypass solutions are proposed. So, we request to change this clause as below:</p> <p>Change Request: "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 external hardware bypass solution from the same OEM as the proposed DDoS mitigation solution."</p> | As per Corrigendum 1                                                                                                                                                                                                                                                                                                                                                                                                               |
| 44 | Section 5.1 "Technical Specification". Requirement "Network Interfaces" /<br><br>( Sr-11 / Page# 17)                     | Minimum 16 x 10GE/25GE SFP28 ports for management and monitoring.                                                                                                                                                                                                                                  | <p><b>Prebid Query / Justification:</b> We do not need more than two out of band ports for management and monitoring.</p> <p><b>Change request :</b> We request to change clause as "<b>minimum 2 x 1GE or 2 x 10GE copper out of band management ports</b>"</p> <p><b>Clarification Request:</b> Our understanding is that the Anti-DDoS appliance should have 16 x 10GE or 25GE Fiber ports for the management/monitoring of the resources/services/applications traffic to be protected and 2 x 10G copper ports are the out-of-band ports for the device management, please confirm.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Section 5.1 revised Sr. 11. minimum 16 x 10GE/25GE SFP28 ports for management and monitoring. additionally, 2 x 1GE or 2 x 10GE copper out of band management ports.                                                                                                                                                                                                                                                               |
| 45 | 5.1 Platform Architecture Requirements<br><br>(Sr - 6 / Page 16) Maximum Sessions Concurrent Attack                      | Unlimited no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections.<br><br>Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks. | <p><b>Justification:</b> Industry standard practice for Anti-DDoS protection of all types of DDoS attacks including L7 attacks is to utilize Stateless Inspection. Including "state/connection tables" as indicated in this point makes the Anti-DDoS appliance Stateful and thereby vulnerable to State Exhaustion Attacks there by defeating the purpose of having an Anti-DDoS appliance. The objective of protecting against the L7 attacks can be effectively achieved using various other stateless countermeasures. So, we request to modify this clause as below:</p> <p><b>Change Request:</b> "Unlimited no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections.<br/><br/>Unlimited concurrent sessions for stateless volumetric mitigation, with either dedicated state/connection tables available for L7 proxy challenges and authentication checks or equivalent countermeasures for bot and advanced application layer DDoS attack protection."</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Section 5.1 Sr 6 Revised: Unlimited — no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections.<br><br>Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks <b>or equivalent countermeasures for bot and advanced application layer DDoS attack protection."</b> |

|    |                       |                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                     |                                                                                                                                                                      |
|----|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46 | Clause 4.2.5, page 13 | 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 quality of implementation and operations by OEM itself of CPU utilization, database activities , OS status etc.          | OEM will require remote access to perform health check and assessment as per the frequency request in RFP. Request you to confirm availability of remote access                                                                     | As per Corrigendum 1                                                                                                                                                 |
| 47 | Clause 4.2.5, page 13 | 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. | Please clarify, if this is expected from ISV/bidder or OEM                                                                                                                                                                          | As per Corrigendum 1                                                                                                                                                 |
| 48 |                       | The SELECTED BIDDER to deploy their OEM certified manpower operations team on-site once implementation gets completed, for 5 years to ensure stabilization and smooth operation & maintenance of the solution. This service to be provided at no additional cost to the tenderer.                                          | Please clarify if you are requesting for Resident Engineer or 24/7 operations desk                                                                                                                                                  | As per RFP                                                                                                                                                           |
| 49 | Clause 7.1, page 26   | PENALTIES FOR ONSITE SUPPORT<br>1. Onsite personnel not present within 1 hour when required (beyond regular timing)                                                                                                                                                                                                        | We request you to clarify if the personnel needs to be present at service desk within one hour? As the request is for beyond regular timing, we request you relax this clause. Professional may not be near to site / occupied etc. | As per RFP                                                                                                                                                           |
| 50 | Clause 7.1, page 26   | 3 Replacement not provided within 30 days (if Tenderer requests)                                                                                                                                                                                                                                                           | We request you to relax this clause as recruitment or redeployment of resources requires additional time. We request to change it to 90 days                                                                                        | As per RFP                                                                                                                                                           |
| 51 | Clause 7.1, page 25   | Malfunctioning of appliances, hardware, hardware components accessories, systems software, or any products, the relevant defect should be attended immediately and rectified within 4 hours of the receipt/notice of the complaint                                                                                         | Time to pick-up/arrange hardware should be excluded, unless spares are kept at near by location                                                                                                                                     | As per RFP                                                                                                                                                           |
| 52 | Clause 4.1, page 11   | 5-year comprehensive onsite warranty from Go-Live.                                                                                                                                                                                                                                                                         | Kindly consider 5-year comprehensive onsite warranty from date of delivery.                                                                                                                                                         | As per RFP                                                                                                                                                           |
| 53 | Clause 5.1, page 17   | Physical Hardware Specifics:<br>Specifically mandates 16 x 10 GigE bypass ports (LR or SR) fiber ports, and hot-swappable dual power supplies.                                                                                                                                                                             | We understand that solution can be meet with higher capacity ports as well. Kindly confirm.                                                                                                                                         | As per Corrigendum 1                                                                                                                                                 |
| 54 | Clause 5.1, page 17   | Network Interfaces:<br>minimum 16 x 10GE/25GE SFP28 ports for management and monitoring.                                                                                                                                                                                                                                   | We understand that solution can be meet with higher capacity ports as well. Kindly confirm.                                                                                                                                         | Section 5.1 revised Sr. 11. minimum 16 x 10GE/25GE SFP28 ports for management and monitoring. additionally, 2 x 1GE or 2 x 10GE copper out of band management ports. |

|    |                       |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 55 | Clause 5.1, page 17   | Maximum Concurrent Attack Sessions: Unlimited — no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections.                                                                                                    | As with all hardware and software, there are limitations based on available memory and compute resources. However, Defender supports a maximum of 2,000 concurrent active events, fully aligned with the defined DCU specifications. This is consistent with industry practices, where both detection and mitigation processes consume compute resources; therefore, unlimited capacity is not feasible<br>Changes Required :<br>Maximum Concurrent Attack Sessions: 2K session state maintained per DDoS mitigation flow. Must handle 2K concurrent attack connections.                                                                                                                                                   | Section 5.1 Sr 6 Revised: Unlimited — no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections. Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks <b>or equivalent countermeasures for bot and advanced application layer DDoS attack protection."</b> |
| 56 | Clause 5.1, page 17   | Maximum Concurrent Attack Sessions: Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks.                                                    | As with all hardware and software, there are limitations based on available memory and compute resources. However, Defender supports a maximum of 2,000 concurrent active events, fully aligned with the defined DCU specifications. This is consistent with industry practices, where both detection and mitigation processes consume compute resources; therefore, unlimited capacity is not feasible<br>Changes Required :<br>Maximum Concurrent Attack Sessions: 2K concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks.                                                                                       | Section 5.1 Sr 6 Revised: Unlimited — no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections. Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks <b>or equivalent countermeasures for bot and advanced application layer DDoS attack protection."</b> |
| 57 | Clause 5.2.1, page 17 | IP Fragment Attacks (Teardrop, Ping of Death, Smurf):<br>Fragment reassembly and anomaly detection                                                                                                                                                            | Secure Genome will identify fragments associated with amplifiers and drop these fragments. IP fragment reassembly is usually performed at the destination host machine. However, some intermediate devices, such as IPS/IDS solutions, may perform fragment reassembly to identify packets that have been fragmented into different components to evade security inspection.<br>Anti-DDoS architecture components are not related to IPS/IDS functionality. Deepfield DDoS components can identify anomalies and perform anomaly detection and mitigation of fragments attack only.<br>Changes Required :<br>IP Fragment Attacks (Teardrop, Ping of Death, Smurf):<br><del>Fragment reassembly</del> and anomaly detection | As per RFP                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 58 | Clause 5.1, page 17   | External Intelligent Bypass/Fail-Open: 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 brought by the bidder if any. | Different OEMs have different ways to fulfill the solution requirement. OEM can give an active/active HW setup with anycast IP for any offramps of DDoS traffic for mitigation, which will work in case of appliance failure. Kindly allow alternative option for more participation.<br>Changes required : 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 brought by the bidder if any or// Offramp Active/Active HW Setup with Anycast IP                                                                                                                                      | As per Corrigendum 1                                                                                                                                                                                                                                                                                                                                                                                                        |
| 59 | Clause 5.2.2, page 18 | HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, CAPTCHA challenge, rate limiting per source IP                                                                                                                                                   | The HTTP server countermeasure inspects all TCP packets submitted to it. Packets with zero payload are passed through, while packets carrying payload data are inspected to identify HTTP requests and HTTP request payload data. The solution countermeasures include fingerprints from Secure Genome technology, has per-source rate limits, sessions limits and idle timeouts. CAPTCHA challenge is hosted on website and usually part of WAF solution. WAF controls the malicious bots for Captcha challenges. Kindly modify the clause and allow more participation.<br>Changes Required:<br>HTTP/HTTPS GET / POST Flood (L7): Behavioral fingerprinting, CAPTCHA challenge, rate limiting per source IP              | As per Corrigendum 1                                                                                                                                                                                                                                                                                                                                                                                                        |

|    |                       |                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                      |
|----|-----------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 60 | Clause 5.2.2, page 18 | DNS Amplification / DNS Water Torture:<br>DNS response rate limiting (DNRRL),<br>query type filtering                   | <p>Solution provides DNS server protection capabilities and offers multiple configurable controls to authenticate and allow traffic from trusted sources. In addition, the solution supports traffic filtering using expressions and FQDN lists. DNS query rates can also be rate limited both toward protected destinations and on a per-source basis to mitigate excessive or malicious query activity. All the response going to DNS need to limit. Solution can also have simultaneous counter measure to turn on to mitigate DNS responses to the victim i.e. Anti-spoofing counter measure.</p> <p>Built-in RRL features inside your DNS server software track requests from specific IP blocks and drop or truncate responses if they exceed safe thresholds as well query type filtering. We request you to amend the clause.</p> <p>Changes Required:<br/>DNS Amplification / DNS Water Torture:<br/><del>DNS response rate limiting (DNRRL), query type filtering</del></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per RFP           |
| 61 | Clause 5.2.2, page 18 | DNS Query Flood (Recursive, NXDOMAIN, ANY):<br>DNS rate limiting Per IP / subnet, source rate thresholds, DNS challenge | <p>DNS query floods can be mitigated through known signatures. Using unscoped filtering, DDoS supports rate limits per source sending DNS queries to the protected destination. DDoS Appliance is not a DNS server hence will not support and response to DNS challenge, but however DDoS can issue a challenge to the requests seen through a name server redirect. Kindly modify the clause.</p> <p>Changes Required:<br/>DNS Query Flood (Recursive, NXDOMAIN, ANY):<br/>DNS rate limiting Per IP / subnet, source rate thresholds,<del>DNS challenge</del></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | As per RFP           |
| 62 | Clause 5.2.2, page 18 | BGP / Routing Protocol Attacks:<br>Control plane protection; BGP session rate limiting                                  | <p>Solution can differentiate between legitimate and malformed traffic using the Invalid Packet Defense mechanism and not defined specific Routing Protocol. Control Plane Protection (CoPP) is usually implemented at the router level as a policy to protect the control plane from being overwhelmed by control plane traffic, such as OSPF, LDP, and BGP, among others.</p> <p>BGP requires TCP port 179, among other components, for the session to be successfully established. It is expected that when a BGP protocol match is configured in CoPP, all control packets matching the classification will be subject to the appropriate action.</p> <p>DDoS can provide the customer with the option to detect traffic destined for TCP port 179 arriving from international boundaries as potentially suspicious traffic attempting to establish a BGP session. DDoS can also provide the option to mitigate such traffic using a custom filter based on TCP port 179 if the requirement indicates that this is necessary.</p> <p>To implement Control-Plane Protection (CoPP) and BGP Session Rate Limiting, you must configure security policies directly on your core routers to protect the router's CPU from being overwhelmed by malicious or excessive network traffic. Kindly make the clause optional or delete it and wider OEM participation</p> <p>Changes Required:<br/><del>Control plane protection and BGP session rate limiting.</del></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | As per Corrigendum 1 |
| 63 | Clause 5.2.2, page 18 | SSL/TLS Exhaustion Attacks:<br>Hardware TLS acceleration for inspection; TLS handshake rate limiting                    | <p>Solution supports multiple TLS server protection mechanisms, including concurrent TLS handshake limiting, Client Hello filtering, and fingerprint-based filtering. These capabilities are applied on a per-protected-object and per-source basis, enabling granular control and protection. Solution provides protection against slow attacks through the TCP Server Protection countermeasure, which incorporates a configurable inactivity timeout to detect and mitigate idle or long-lived malicious connections. Deepfield is a detection and mitigation solution, and there is no additional hardware for inspecting TLS packets through decryption and subsequent re-encryption. The majority of attacks today originate from botnets, and the objective of inspection is often to identify whether malware is concealed within the encrypted traffic.</p> <p>Although DDoS does not provide decryption or encryption hardware for traffic inspection, it can identify the majority of known bots based on years of research and accumulated intelligence. This provides an alternative approach for the Internet today, where the majority of traffic is encrypted. Deploying hardware to decrypt and re-encrypt traffic at large scale can introduce scaling challenges over time.</p> <p>The modern approach implemented by Deepfield is to identify and mitigate known bots, thereby addressing the source of the attack directly. This is a more practical alternative to deploying hardware for TLS inspection and performing decryption and re-encryption, particularly because the customer would also need to have access to the relevant keys, which may not be readily available for all sources communicating with the destination. TLS acceleration is known as SSL Termination. The load balancer handles the heavy cryptographic processing using specialized internal hardware chips (ASICs), decrypts the traffic, and forwards plain HTTP traffic to the backend servers. However, if a massive TLS flood attack occurs, the load balancer's CPU will be the primary target of exhaustion. TLS acceleration is not DDoS attack and It must be manage by Application Load balancer.</p> <p>Changes Required:<br/>SSL/TLS Exhaustion Attacks:<br/><del>Hardware TLS acceleration for inspection;</del> TLS handshake rate limiting</p> | As per Corrigendum 1 |

|    |                       |                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                      |
|----|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 64 | Clause 5.2.3, page 18 | HTTP/HTTPS DDoS Protection:<br>Deep HTTP inspection, URL rate limiting, method filtering (GET/POST/HEAD), User-Agent filtering                                   | <p>The solution provides HTTP Server Protection capabilities to safeguard web servers against application-layer DDoS attacks. Protection against HTTP-based attacks is applied to the configured service ports. The solution performs HTTP protocol validation by dropping malformed or non-compliant HTTP messages. It also supports HTTP source authentication through redirect-based challenges containing authentication tokens embedded within the URL. HTTP clients that successfully process the redirect and return the token in subsequent requests are validated as legitimate sources. To control excessive traffic, the solution supports HTTP GET and POST request rate limiting. Rate limits may be configured globally for the protected object or individually on a per-source basis. URL rate limiting and user-agent filtering is IPS/IDS solution. Using a Web Application Firewall (WAF) stops unwanted User-Agents before they ever hit your web servers and URL rate limiting. Kindly modify the clause and allow more participation.</p> <p>Changes Required:<br/>HTTP/HTTPS DDoS Protection:<br/>Deep HTTP inspection, <del>URL rate limiting, method filtering (GET/POST/HEAD), User-Agent filtering</del></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | As per Corrigendum 1 |
| 65 | Clause 5.2.3, page 18 | SSL/TLS Decryption for DDoS:<br>Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS | <p>The solution provides TLS Server Protection capabilities to safeguard TLS-based servers against application-layer DDoS attacks. Protection against TLS-based attacks is applied to the configured service ports. The solution performs TLS protocol validation by dropping malformed or non-compliant TLS messages.</p> <p>To mitigate TLS handshake exhaustion attacks, the solution supports concurrent TLS handshake limiting. Maximum concurrent handshake thresholds may be enforced globally for the protected object or individually on a per-source basis.</p> <p>The solution also supports TLS Client Hello filtering to prevent attacks that leverage excessively complex handshake requests. Configurable limits may be applied to the number of cipher suites and extensions contained within Client Hello messages. Messages exceeding the configured thresholds are discarded.</p> <p>In addition, the solution supports TLS fingerprint filtering based on JA3 and JA4 fingerprints. TLS Client Hello messages are evaluated against user-defined fingerprint lists, and matching clients may be either permitted or blocked. A default action can also be defined for fingerprints that do not match any configured list, allowing non-matching clients to be either dropped or further evaluated by other protection mechanisms.</p> <p>The solution does not support TLS/SSL payload decryption. This architectural design preserves end-to-end encryption and eliminates the need to store or manage customer certificates and private keys, thereby reducing security and operational risks.</p> <p>SSL/TLS decryption is not part of DDoS solution and IPS/IDS is required for SSL/TLS Decryption and deep inspection. Kindly modify the clause and allow more OEM participation.</p> <p>Changes Required:<br/>SSL/TLS Decryption for DDoS:<br/>Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS or//TLS protocol messages validation, Mitigate TLS handshake exhaustion attack, TLS fingerprint filtering based on JA3 and JA4 fingerprints</p> | As per Corrigendum 1 |
| 66 |                       | DNS Protection:<br>DNS rate limiting per source, DNSSEC support, malformed DNS drop, RD flag filtering, TTL manipulation detection                               | <p>DNSSEC is a DNS security extension that is implemented and supported by DNS servers and resolvers. The RD flag is a bit in the DNS query header that indicates whether the client is requesting the DNS server to perform recursive resolution. Both are settings or capabilities that can be found in DNS servers, where DNSSEC is used to validate DNS queries and responses, while the RD flag indicates whether recursive resolution is requested.</p> <p>Apart from the DNS server-specific features, DDoS can apply rate limiting on a per-source basis, allowing DNS queries to be limited to a specified number of queries per second towards the protected destinations.</p> <p>DDoS can also identify and drop oversized or irregular DNS packets that are non-conformant, using Secure Genome technology, where signatures are appended to flow records to identify the source of the DNS traffic and determine whether the source is compromised. In addition, DDoS provides TTL manipulation detection through its anti-spoofing countermeasure.</p> <p>DDoS is not a DNS server by nature and, therefore, does not support the DNS server-specific features as mentioned above.</p> <p>Changes Required:<br/>DNS Protection:<br/>DNS rate limiting per source, DNSSEC support, malformed DNS drop, RD flag filtering, TTL manipulation detection</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | As per RFP           |

|    |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                        |
|----|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 67 | Clause 5.2.3, page 18 | API Protection:<br>Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection                                                                                                                                                                                                                                                                                                                                                                                                                               | The solution provides multiple protection mechanisms, including rate limiting, which can be applied to control requests directed toward API endpoints. In addition, the solution is capable of detecting and mitigating anomalous traffic patterns through the TLS protection mechanisms described above. Inspecting all of these elements requires the decryption and re-encryption of Internet traffic. As everyone is aware, the Internet today is extremely large in scale, and the majority of traffic is encrypted. DDoS recognizes that the root cause of much of this modern warfare originates from the source and therefore focuses on identifying and mitigating the source of the threat directly, rather than following the market trend of building decryption and encryption hardware that may not be utilized at all and could result in unnecessary expenditure for customers.<br>The Deepfield approach is focused on efficiency in terms of detecting and mitigating DDoS attacks in today's modern Internet environment.<br>Changes Required:<br>API Protection:<br>Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection Or// API running on 443 protection | As per Corrigendum 1                                                   |
| 68 | Clause 5.3, page 19   | False Positive Rate:<br>Bidder to demonstrate false positive rate of < 1% in reference deployments.                                                                                                                                                                                                                                                                                                                                                                                                                    | A DDoS false positive occurs when legitimate customer traffic is incorrectly flagged and blocked as a Distributed Denial of Service attack. 5 % is the industry standard, legitimate traffic is being dropped. Kindly modify the clause.<br>Changes Required :<br>False Positive Rate:<br>Bidder to demonstrate false positive rate of < 5% in reference deployments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per Corrigendum 1                                                   |
| 69 | Clause 5.4, page 20   | On-Demand / Out-of- Path Scrubbing: BGP diversion: traffic rerouted to appliance scrubbing center during detected attacks; clean traffic re-injected via GRE / IPsec tunnel or policy-based routing.                                                                                                                                                                                                                                                                                                                   | We support an out-of-path scrubbing deployment model, where FlowSpec redirection is used to off-ramp DDoS traffic to the mitigation device. We understand that malformed or attacked traffic is rerouted to on-premise mitigation facility for scrubbing. Kindly confirm that our understanding is correct.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | As per Corrigendum 1                                                   |
| 70 | Clause 5.5, page 21   | Application-Level Bypass & Fail-Safe Mechanisms:<br>The solution must provide an 'Application-Level Bypass' functionality, allowing the administrator to exempt specific application traffic from mitigation engines in real-time without taking the entire appliance offline. Furthermore, the appliance must support 'Fail-to-Wire' (physical bypass) capabilities, ensuring that in the event of hardware or software failure, the network link remains operational (traffic is passed through without inspection). | Different OEMs have different ways to fulfil the solution requirement. There can be a active/active DMS setup with anycast IP for any offramps of DDoS traffic for mitigation.<br>Changes Required:<br>Application-Level Bypass & Fail-Safe Mechanisms:<br>The solution must provide an 'Application-Level Bypass' functionality, allowing the administrator to exempt specific application traffic from mitigation engines in real-time without taking the entire appliance offline. Furthermore, the appliance must support 'Fail-to-Wire' (physical bypass) capabilities, ensuring that in the event of hardware or software failure, the network link remains operational (traffic is passed through without inspection). or// Offramp Active/Active Setup with Anycast IP                                                                                                                                                                                                                                                                                                                                                                                                                   | As per Corrigendum 1                                                   |
| 71 | Clause 5.5, page 21   | Operating Temperature: 0°C to 40°C; Humidity: 10% to 90% non-condensing                                                                                                                                                                                                                                                                                                                                                                                                                                                | Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5°C to 40°C; Humidity: 10% to 90% non-condensing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | As per RFP                                                             |
| 72 | Clause 4.2.1, page 11 | Power Supply redundancy: dual redundant hot-swappable PSUs                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Kindly confirm the type of power supply AC or DC required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | As per RFP                                                             |
| 73 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | How many Peering Router DC and kindly share the Make and Model ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | if require bidder may conduct site visit to understand existing infra. |
| 74 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Peering Router Traffic handling capacity ? Internet or external Traffic?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | if require bidder may conduct site visit to understand existing infra. |
| 75 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | What will be the sampling rate ? 5/1000 packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | As per RFP                                                             |
| 76 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | What is the peak internet bandwidth your current data center handles?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | As per RFP                                                             |
| 77 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Are we planning to non-web protocols (like TCP/UDP gaming, proprietary apps) and protecting web-based traffic (HTTP/HTTPS) or?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | As per RFP                                                             |
| 78 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Are you looking to protect an on-premises data center or a cloud-hosted application?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | As per RFP                                                             |
| 79 | NA                    | Additional Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | This Anti-DDoS solution opportunity is only for GSDC at DC location or DC and DR location. Kindly Confirm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | only DC location                                                       |