| Response to Pre-Bid Queries for RFP | | | | | |
|---|---|---|---|---|---|
| **RFP Ref. No.** | | **CPCM-07/2025-26 Date: 02-July-2025 GEM Bid No. GEM/2025/B/6402236** | | | |
| **RFP Name** | | **RFP for Procurement of Cloud based Web Application and API Protection (WAAP)** | | | |
| **Sr. No.** | **Page No.** | **RFP Clause** | **Clause Description** | **Query** | **StockHolding Remarks** |
| 1 | 8 | Eligility Criteria | Bidder should have an average annual turnover of at least ₹ 2.8 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of should be of individual company and not of Group of Companies | The requested turnover asked for Bidder is very less. To ensure the right partipation, We requsest Turnover should be minimum 30 Crores per annum. Hence Revised suggested clause: Bidder should have an average annual turnover of at least ₹ 30 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of should be of individual company and not of Group of Companies | No Change. Same as RFP. |
| 2 | 8 | Eligility Criteria | The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | Kindly confirm if the reference from Bidder asked is for the proposed Cloud WAAP only and not for an on prem WAF solution | Bidder to submit reference only for proposed cloud WAAP. |
| 3 | 57 | ANNEXURE – 10 – Technical Compliance | The entire solution must be centrally managed for day to day operations. Reporting, policy creation, alerts management, web application protection configuration, etc must be managed from the management server | Kindly clarify if the central management should be common and a single dashboard to manage apps for both internal WAF and Cloud WAAP | **Clarification:** Central Management should be common and a single dashboard to manage Apps for both internal WAF and Cloud WAAP |
| 4 | 48 | ANNEXURE – 10 – Technical Compliance | Proposed Solution must be a SaaS offering for WAAP (web application & api protection) along with DDOS ( L3/L4 and L7 ) with client side defense & Bot Defense from single platform | Referring to Annex 4, there is no subscribtion line item of BOT Defence. Would like to know if Bot Defence is required from day1 or OEM just need to comply as per available service offering and BOT defense can procured in the future with a license addon? | **Clarification:** BOT Defence should should be available from Day 1 within the commercials |
| 5 | 53 | ANNEXURE – 10 – Technical Compliance | The solution must be able to perform virtual patching for its protected web applications. | Requesting Stock Holding to clarify whether virtual patching refers to rule-based mitigation at Layer 7 (e.g., WAF signatures, custom policies) or includes OS/application-level vulnerability shielding, as the scope needs to be clearly defined for a cloud WAAP solution. | **Clarification:** Virtual patching refers to Layer 7 rule-based mitigation mechanisms, such as WAF signatures and custom detection rules, that provide immediate protection against known application-layer vulnerabilities without requiring changes to the application source code or server environment.” |
| 6 | 58 | ANNEXURE – 10 – Technical Compliance | (East-West Traffic) Internal Web Application Firewall | OEM would need more details with regards to East-West traffic for WAF. How many application need to be protected behind on-prem WAF? Is it only WAF or would need API Security as well? Also kindly confirm the nof of sites to deploy on prem WAF | **Clarification:** Approximately 100 servers at DC site and approximately 50 servers at DR site needs to be behind internal WAF. There are no internal API's to be monitored, however it may be introduced in the near future |
| 7 | NA | General Queries | General Queries | Kindly request Stock Holding to provide the approximate number of API connections per month. This data is critical for bidders to accurately size the Bill of Quantity (BOQ) and infrastructure requirements for both East-West and North-South traffic patterns. | **Clarification:** There are Approximately 2 Crore API specific connections per month combining all the mentioned domains. However we understand all the requests url's for the mentioned domains has to be scanned. |
| 8 | NA | General Queries | General Queries | Kindly confirm the no of Dynamically and continuously scan to be included for external attack surface to un-cover exposed web apps and APIs. | **Clarification:** No (webapps and API's) to be un-covered |
| 9 | 16 | Scope Of Work | DNS Security: Use DNSSEC to secure DNS queries | Kindly confirm the no of primary and/or secondary zones to be included in the BOQ to be supported which should support DNS SEC as part of the solution | **Clarification:** Platform shall support multiple primary/secondary zones. Exact information shall be shared with the selected bidder |
| 10 | 8 | Eligility Criteria | The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | Request you to kindly revise the clause as per below-<br><br>The bidder should have at least 03 (three) successful implementations in India of WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | No Change. Same as RFP. |

| | | | | | |
|---|---|---|---|---|---|
| 11 | 8 | Eligility Criteria | Bidder should have an average annual turnover of at least ₹ 2.8 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of should be of individual company and not of Group of Companies | The requested turnover asked for Bidder is very less. To ensure the right partipation, We requsest Turnover should be minimum 30 Crores per annum. Hence Revised suggested clause: Bidder should have an average annual turnover of at least ₹ 30 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of should be of individual company and not of Group of Companies | No Change. Same as RFP. |
| 12 | 11 | Technical Criteria | OEM solution must be positioned in the Leaders Quadrant of the latest IDC MarketScape, Gartner Magic Quadrant, or Forrester Wave reports for Web Application Firewall and API Protection. | Gartner has stopped publishing reports for WAAP since 2022. Request to include other leading Analysts like QKS SPARK Matrix or GigaOm for WAAP. Request to change the clause as per below:<br>"OEM solution must be positioned in the Leaders or Major player Quadrant of the latest IDC MarketScape or QKS Spark Matrix, or GigaOm or Forrester Wave reports for Web Application Firewall and API Protection. | No Change. Same as RFP. |
| 13 | 56 | ANNEXURE – 10 – Technical Compliance | There should be centralized Monitoring and Management station with capability for log collection for minimum 180 days | Request to change as per below :<br>"There should be centralized Monitoring and Management station with capability for log collection for minimum 90 days" | No Change. Same as RFP. |
| 14 | 53 | ANNEXURE – 10 – Technical Compliance | The solution must be able to perform virtual patching for its protected web applications. | Requesting Stock Holding to clarify whether virtual patching refers to rule-based mitigation at Layer 7 (e.g., WAF signatures, custom policies) or includes OS/application-level vulnerability shielding, as the scope needs to be clearly defined for a cloud WAAP solution. | **Clarification:**<br>Virtual patching refers to Layer 7 rule-based mitigation mechanisms, such as WAF signatures and custom detection rules, that provide immediate protection against known application-layer vulnerabilities without requiring changes to the application source code or server environment.” |
| 15 | 14 | Scope Of Work - A. Task & Deliveries | Supply, installation and commissioning of Cloud based WAF and DDOS service with clean bandwidth of 50Mbps/15TB/month. | Break-up of Throughput for Cloud WAF (external) and On-Prem WAF (Internal) | **Clarification:**<br>We do not have Cloud WAF now. RFP clearly mentions about migrating from On-Premise WAF to Cloud WAAP. |
| 16 | 17 | 19) Assessment & Planning | Define a timeline and plan for the migration process with minimal downtime 20) Cloud WAF Configuration | Please specify 20 as number of days or weeks | **Clarification:**<br>RFP says "Define a timeline and plan for the migration process with minimal downtime." This has to be envisaged and planned by the selected bidder |
| 17 | 14 | Scope Of Work | Migration of on Prem WAF to Cloud WAF | Request to share High Level Architecture for detailed scope of work and clarity | **Clarification:**<br>Will be shared with winning bidder |
| 18 | 14 | Scope Of Work | OEM should have WAF services hosted from India Data center only | Please confirm if any other considerations need to be made for the DC or any DC within India can be used for hosting the solution | **Clarification:**<br>Within India any DC will do |
| 19 | 8 | Eligility Criteria | The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP dat | Kindly Modify as:<br>The bidder/OEM should have at least 03 (three) successful implementations in India of the proposed WAF/WAAP solution of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | No Change. Same as RFP. |
| 20 | 8 | Eligility Criteria | OEM should have WAF services hosted from India Data center only | Clause to be added as Cloud WAAP solution to be hosted on a MEITY empaneled DC to meet regulatory guidelines | No Change. Same as RFP. |
| 21 | 3 | Interest free Earnest Money Deposit (EMD) [*] | Rs.10,50,000/- (Indian Rupees Ten Lakhs Fifty Thousand only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as<br>Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on StockHolding’s Bank<br>Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address. | EMD exemption to bidders as per GeM GTC | EMD exempted for MSME bidders |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 11 | Technical Bid Evaluation (Stage 2) | OEM solution must be positioned in the Leaders Quadrant of the latest IDC MarketScape, Gartner Magic Quadrant, or Forrester Wave reports for Web Application Firewall and API Protection. | Gartner has stopped publishing reports for WAAP since 2022. Request to include other leading Analysts like QKS SPARK Matrix or GigaOm for WAAP. Request to change the clause as per below:<br>"OEM solution must be positioned in the Leaders or Major player Quadrant of the latest IDC MarketScape or QKS Spark Matrix, or GigaOm or Forrester Wave reports for Web Application Firewall and API Protection. | No Change |
| 23 | 56 | Monitoring, Logging & Reporting | There should be centralized Monitoring and Management station with capability for log collection for minimum 180 days | Request to change as per below :<br>"There should be centralized Monitoring and Management station with capability for log collection for minimum 90 days" | No Change |
| 24 | 29 | ANNEXURE - 3 – Technical Criteria | The bidder should have at least 03 (three) successful implementations in India of the WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | Request to change as per below :<br>"The bidder should have at least 03 (three) successful implementations in India of the WAAP solution of the proposed OEM or similar Product OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | No Change. Same as RFP. |
| 25 | 29 | ANNEXURE - 3 – Technical Criteria | • 3 projects : 10 Marks<br>• 4-5 Projects: 15 marks<br>• More than 5 Projects: 20 Marks | Request to change as per below :<br>• 3 projects : 15 Marks<br>• 4-5 Projects: 20 marks | No Change. Same as RFP. |
| 26 | 20 | Service level and Penalty | Uptime of WAF should be 99.9% on monthly basis. Partial or full unavailability of WAF shall be treated as downtime. | Request to change as per below :<br>Uptime of WAF should be 99.999% on monthly basis. | No Change |
| 27 | 58 | ANNEXURE – 10 – Technical Compliance | The solution must support virtual patching for known vulnerabilities without requiring changes to application code. | Suggestion:<br>There are higher chances of false positive with Virtual Patching since these patches are untested.<br><br>Hence requesting you to kindly remove this point. | No Change |
| 28 | 58 | ANNEXURE – 10 – Technical Compliance | The solution must be able to perform virtual patching for its protected web applications | Suggestion:<br>There are higher chances of false positive with Virtual Patching since these patches are untested.<br><br>Hence requesting you to kindly remove this point. | No Change |
| 29 | 60 | ANNEXURE – 10 – Technical Compliance | The solution should also support sending of logs in CEF (Common Event Format) standard | CEF is a legacy format. It is recommended to use more advanced and latest JSON format.<br><br>Hence requesting you to kindly add below point:<br>The solution should also support sending of logs in JSON format | **Clarification:**<br>CEF format is required for SIEM log data ingestion.<br>No change |
| 30 | 8 | Eligility Criteria | The proposed OEM should have ISO 27000 and/or SOC2 Type2 series certifications | Request to change as per below :<br>The proposed OEM should have ISO 27001<br>ISO 27701<br>ISO 27017<br>ISO 27018<br>ISO 27032<br>ISO 28000<br>EU GDPR<br>PCI-DSS<br>HIPAA<br>US SSAE16 SOC-1 Type II, SOC-2 Type II | No Change |
| 31 | NA | Suggestion for Addition of Clause | Suggestion for Addition of Clause | Solution should be able to support custom/non-standard ports for any application. | No Change to RFP clauses |
| 32 | NA | Suggestion for Addition of Clause | Suggestion for Addition of Clause | With the adoption of native mobile applications, cyber attackers using bots have found another attack surface to exploit. Without attestation, it is extremely difficult to validate whether a request to access an application originated from a real device.<br>The attestation feature ensures that only real devices and authentic applications can access requested resources.<br><br>Hence requesting you to kindly add below point:<br>Solution should support mobile attestation for both iOS & Android devices to prevent BOT attacks on mobile devices | No Change to RFP clauses |

| | | | | | |
|---|---|---|---|---|---|
| 33 | NA | Suggestion for Addition of Clause | Suggestion for Addition of Clause | It is key to have load balancing between multiple origin servers for high availability<br>Hence requesting you to kindly add below point:<br>"Load Balancing between origin servers and DC-DR" | No Change to RFP clauses |
| 34 | NA | Suggestion for Addition of Clause | Suggestion for Addition of Clause | | No Change to RFP clauses |
| 35 | 8 | Eligility Criteria | The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP dat | Kindly Modify as:<br>The bidder/OEM should have at least 03 (three) successful implementations in India of the proposed WAF/WAAP solution of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date | No Change. Same as RFP. |