| Corrigendum – Tender Reference No.: DGRPG/PSDC_DCO/2023/2 | | | | | |
|---|---|---|---|---|---|
| **SN** | **Tender / ATC Clause No.** | **Page No.** | **Tender / ATC Clause** | **Tender / ATC clause details / specification** | **Revised Clause** |
| 1 | 11.1.11 | 94 | Payment Terms - General | Additional Clause | All payments to the Service provider shall be made within 45 days after auditing and calculations by the Third Party Auditor appointed by DGRPG. |
| 2 | 7.5.1.24 | 72 | Roles and Responsibility | **Activity** - Recurring expenditure **like electricity, diesel**, after implementation during the Operation and Maintenance Phase<br>**DGRPG** - Yes<br>**DCO** - Yes<br>**TPA** - Yes<br>**Remarks** - * On actual consumption, "During post implementation, the recurring expenses **towards diesel and electricity** would be on actual basis & shall be paid to the DCO by **the SG** on a quarterly basis."<br>The amount to the DCO will be reimbursed in actual and NO service TAX will be added by the DCO onto it.<br>*Operational expenses **(Electricity and Diesel)** during Implementation would also be on actual consumption and shall be paid to the DCO by DGRPG on a quarterly basis. | **Activity** - Recurring expenditure **like diesel**, after implementation during the Operation and Maintenance Phase<br>**DGRPG** - Yes<br>**DCO** - Yes<br>**TPA** - Yes<br>**Remarks** - * On actual consumption, "During post implementation, the recurring expenses **towards diesel** would be on actual basis & shall be paid to the DCO by **DGRPG** on a quarterly basis."<br>The amount to the DCO will be reimbursed in actual and NO service TAX will be added by the DCO onto it.<br>*Operational expenses **(Diesel)** during Implementation would also be on actual consumption and shall be paid to the DCO by DGRPG on a quarterly basis. |
| 3 | 7.5.1.25 | 72 | Roles and Responsibility | **Activity** - Obtain regulatory and other clearances for setting up the extended Data Centre.<br>**DGRPG** - Yes<br>**Remarks** - State government will facilitate requisite documentation from its end; however, DCO shall have liaison & coordinate with the relevant agencies for getting the clearances and approvals. | Clause stands deleted. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 9.9 | 80 | Project Implementation and Payment Schedule | All payments shall be made corresponding to the goods or services delivered, installed, or operationally accepted, **per the Contract implementation Plan**, at unit prices and in the currencies specified in the Financial Bid. | All payments shall be made corresponding to the goods or services delivered, installed, or operationally accepted, **as per clause no. - 9.1**, at unit prices and in the currencies specified in the Financial Bid. |
| 5 | 6.11.1 | 30 | Subcontracting by Data Centre Operator | **The service provider may subcontract non-IT work. Subcontracting of IT resources may be allowed** after approval of DGRPG, however, resources to be subcontracted will be at the sole discretion of DGRPG. However, the service provider shall provide the list of services planned to be subcontracted, within 45 days of signing the Agreement or at least 45 days before the start of proposed subcontracted work whichever is later. | **The service provider may subcontract non-IT & IT work. However, sub contracting of IT manpower may be allowed only after approval of DGRPG. The** service provider shall provide the list of services planned to be subcontracted, within 45 days of signing the Agreement or at least 45 days before the start of proposed subcontracted work whichever is later. |
| 6 | 10.7.g.2 | 91 | SI/FM Manpower Availability - Availability of Project In-Charge/ Project Manager | Service Provider needs to ensure that<br>Project In-Charge/ Project Manager shall not take any leave (**Max. leave allowed - 12 in a year**) without prior approval from DGRPG. If resource deployed is not reporting to duty for 3 consecutive days without sanctioned leaves, the same will be treated as non- deployment for the purpose of liquidated damages calculation. | Service Provider needs to ensure that<br>Project In-Charge/ Project Manager shall not take any leave (**Max. leaves allowed - 18 in a year**) without prior approval from DGRPG. If resource deployed is not reporting to duty without sanctioned leaves, the same will be treated as non- deployment for the purpose of liquidated damages calculation. **During leave period, resource should be available on phone or a temporary replacement / remote support to be provided.** |
| 7 | Annexure - B (IT Components). G.1 | 163 | Next Generation Firewall (NGFW) | The solution should have atleast **4 X 1G/10G Cu, 16 X 10G/25G (SFP/ SFP+), 4 X40G/100G (QSFP/ QSFP+)** with all ports fully loaded from day 1. | The solution should have atleast **4 X 1G/10G Cu, 16 X 10G or 25G (SFP/ SFP+), 4 X 40G/100G (QSFP/ QSFP+)** with all ports fully loaded from day 1. |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Annexure - B (Non-IT Components). 14 | 310 | Technical specifications for IPDUs | Intelligent Rack PDU should be 3 phase 16AMP must support 11KW load have minimum 18 no's C13 and 6 no's C19 socket for power distribution to IT equipment and should be mounted vertically in rear of rack occupying 0U space, UL certified. | Intelligent Rack PDU should be 3 phase 16AMP must support 11KW load have minimum 18 no's C13 and 6 no's C19 socket for power distribution to IT equipment and should be mounted vertically in rear of rack occupying 0U space, UL certified. **The PDU shall be able to provide parameters like device, peak, apparent power, power factor, phase voltage, current, peak current, power. The PDU shall support temperature & Humidity sensor. To avoid accidental disloging high retention sockets / lockable power cords shall be provided.** |
| 9 | 11.1.9 | 94 | Payment Terms - General | The Service Provider's cumulative liability to DGPRG under the contract for all claims made under or in connection with the contract whether arising under contract (including under any indemnity), negligence or any other tort, under statute or otherwise at all will not exceed the total contract value in aggregate of the contract. | Clause stands deleted. |
| 10 | 6.14 | 31 | Limitation of Liability | Additional Clause | The Service Provider's cumulative liability to DGPRG under the contract for all claims made under or in connection with the contract whether arising under contract (including under any indemnity), negligence or any other tort, under statute or otherwise at all will not exceed the total contract value in aggregate of the contract. **Further, service provider will not be liable for any indirect or consequential damages which are not forseeable.** |
| 11 | Annexure - B (IT Components). G.10 | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have at least 2TB log capability **internally** along with support for scalable external storage (eg: SAN/RAID) feature. | Firewall Solution should have at least 2TB log capability **internally / externally** along with support for scalable external storage (eg: SAN/RAID) feature. |
| 12 | Annexure - B (IT Components). G.11 | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have inbuilt redundant hot-swappable power supply **and inbuilt hot-swappable/replaceable fans/ tray/ modules.** | Firewall Solution should have inbuilt redundant hot-swappable power supply **and swappable Fans/redundant fans/ tray/ modules.** |

| | | | | | |
|---|---|---|---|---|---|
| 13 | 7.5.1.10 | 70 | Roles and Responsibility | **Activity** - Obtain Electrical & Fire NOC from concerned Departments. DGRPG will assist for the same.<br>**DGRPG** - Yes<br>**DCO** - Yes | Clause stands deleted. |
| 14 | 7.3.2.5.4 | 40 | Next Generation Firewall (NGFW) | PSDC is using Checkpoint 12200 firewall in HA mode **and is required to be upgraded with following configurations**:- 8 x 10/100/1000Base-T RJ45 ports, One network card expansion slot, 8 GB memory, 2 x 500 GB HDD, LOM card, Slide rails (22" to 32"), 1.7 (default)/5(max) million concurrent connections, 90,000 connections per second. | PSDC is using Checkpoint 12200 firewall in HA mode **with following configurations**:- 8 x 10/100/1000Base-T RJ45 ports, One network card expansion slot, 8 GB memory, 2 x 500 GB HDD, LOM card, Slide rails (22" to 32"), 1.7 (default) / 5 (max) million concurrent connections, 90,000 connections per second. |
| 15 | 7.3.2.9 | 42 | Upgradation of the PSDC | The specifications given in Annexure - B for the non-IT components are applicable only in case a new component is required to be installed or existing component is required to be **replaced**. | The specifications given in Annexure - B for the non-IT components are applicable only in case a new component is required to be installed or existing component is required to be **replaced / upgraded**. |
| 16 | Annexure - B (IT components). A.9 | 154 | EMS/NMS Specifications for 05 Years warranty and AMC support | Proposed solution must have at least 3 deployments in Central Government/Public Sector/State Govt./PSU`s/Large Enterprise, out of which one should be in a DC environment, monitoring & managing 10,000+ **nodes/servers/endpoints** across these three deployments. | Proposed solution must have at least 3 deployments in Central Government/Public Sector/State Govt./PSU`s/Large Enterprise, out of which one should be in a DC environment, monitoring & managing 10,000+ **network nodes/servers** across these three deployments. |
| 17 | Annexure - B (IT components). E.1 | 160 | Security Incident Management Solution (SIEM) | Solution should encompass **log, packet and end point data** with added context and threat Intelligence. Should provide complete network visibility through deep inspection of logs | Solution should encompass **log and end point data** with added context and threat Intelligence. Should provide complete network visibility through deep inspection of logs |
| 18 | 4.1.3 | 9 | Introduction | PSDC is **Tier – II Data Centre** and is ISO 20000 & ISO 27001 certified | PSDC is **Tier – II compliant Data Centre** and is ISO 20000 & ISO 27001 certified |

| | | | | | |
|---|---|---|---|---|---|
| 19 | 5.1.2.PQ6 | 11 | Eligibility / pre-qualification criteria | Qualification Criteria - Bidders are required to submit bid specific Manufacturing Authorization Form (MAF) **confirming that the products quoted are neither end of sale nor end of life.**<br><br>Documents/ Information to be provided - **For the OEM's of all IT & non-IT assets to be provided by the bidder.** | Qualification Criteria - Bidders are required to submit bid specific Manufacturing Authorization Form (MAF) **for all IT assets, however, MAF is required for following non - IT assets only:-**<br>**1- Access Control System.**<br>**2 -CCTV Panel**<br>**3 -Fire Suppression System**<br>**4- WLD**<br>**5- CAC**<br>**6- PA System**<br>**7- Aspiratory System**<br><br>Documents/ Information to be provided - **MAF confirming that the products quoted are neither end of sale nor end of life.** |
| 20 | Annexure - B (Non-IT components). 4.C.4.e | 214 | Data Center Infrastructure Management Systems (DCIMS) | Cloud Based Datacenter Remote Monitoring Services to offer second layer of intensive coverage over Threshold Violations, Rules, Alerts arising within the DCIM. This system should have a dedicated manpower NOC from where the DCIM OEM will be handling this Remote Monitoring service. | Cloud Based Datacenter Remote Monitoring Services to offer second layer of intensive coverage over Threshold Violations, Rules, Alerts arising within the DCIM. This system should have a dedicated manpower NOC from where the DCIM OEM will be handling this Remote Monitoring service. **The cloud option must be security hardened with a mandatory two-factor authentication and high encryption standards (2048 bit AES256). It must be committed to comply with its obligations under the GDPR to reduce any chance of Data Breach.** |
| 21 | Annexure - B (Non-IT components). 3.P | 205 | Data Center Infrastructure Management Systems (DCIMS) | UPS shall have built-in features to test UPS at 100% Load without the need of any external Load Bank. In case this feature is not available within the UPS, Vendor shall provide an External Load Bank equal to UPS Capacity **which will be kept at the site till the end of Warranty period.** | UPS shall have built-in feature to test UPS at 100% Load without the need of any external Load Bank. Incase this feature is not available within the UPS, Vendor shall provide an External Load Bank equal to UPS Capacity. |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 7.3.2.5.4.1 | 40 | Next Generation Firewall (NGFW) | Additional Clause | Punjab Wide Area Network (PAWAN) provides the necessary bandwidth for PSDC. PAWAN caters to the external firewall service for the PSDC which is Fortinet Next-Generation firewall (Model - 3601E). With the objective of enhancing security, Service Provider has to deploy internal firewall from different OEM than that of external one. |
| 23 | 5.1.Note | 12 | Eligibility / pre-qualification criteria | Additional point | For PQ4, bidder may submit parent company's PO in case of in-house Data Centres. In such case, parent company will also be made liable in the contract to be signed by the client with the subsdiary.<br>Bidder to submit self declaration for the same from its parent company during bid submission. |

| Response to Queries (RTQ) – Tender Reference No.: DGRPG/PSDC_DCO/2023/2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| **SN** | **Tender / ATC Clause No.** | **Page No.** | **Tender / ATC Clause** | **Tender / ATC clause details/specification** | **Amendment Sought / Suggestion** | **Justification** | **PSeGS response** |
| 1 | 5.1 | 10 | Eligibility / pre-qualification criteria | Bidders should have successfully completed “similar work” in government (departments/ boards/ corporations/ PSUs/ Societies) / Large reputed Enterprise during the last ten years ending 31.03.2023. ● One similar work costing not less than the amount equal to Rs. 30 crore. OR ● Two similar works each costing not less than the amount equal to Rs. 25 crore each. OR ● Three similar works each costing not less than the amount equal to Rs. 15 crore each. Work orders/ documents confirming year, cost, area of activity and other parameters sought in the qualification criteria. Any other relevant documents for costing of each similar work are also acceptable. Ongoing projects with Go Live or FAT Certificate by competent authority from customer/end client or with minimum 2 years of operations can also be considered. Proof of completion of work / satisfactory certificate /proof of payment from CA is to be submitted along with work orders. | **1.** One similar work costing involving a Tier 3 Data Centre.<br>**2.** Please allow parent company's PO to be shown for in house data center.<br>**3.** Bidders should have successfully completed “similar work” in government (departments/ boards/ corporations/ PSUs/ Societies) / Large reputed Enterprise during the last ten years ending 31.03.2023.<br>● One similar work order not less than the amount equal to Rs. 30 crore. OR<br>● Two similar work orders each costing not less than the amount equal to Rs. 25 crore each. OR<br>● Three similar work orders each costing not less than the amount equal to Rs. 15 crore each. Work orders/ documents confirming year, cost, area of activity and other parameters sought in the qualification criteria. Any other relevant documents for costing of each similar work are also acceptable. Ongoing projects with Go Live or FAT Certificate by competent authority from customer/end client or Ongoing projects value would also be consider with latest Completion Certificate of operations can also be considered. Proof of completion of work / satisfactory certificate /proof of payment from CA is to be submitted along with | **1.** As Punjab DCO is going in for Tier 3 certification it is imperative that the selected service provider/SI must have the experience in building/managing a Tier 3 DC.<br>**2.** All POs related to Major DC built are placed thru our Parent Company, so request you to consider<br>**3.** Relevance and Currency of Experience: Including ongoing projects in the tender qualification criteria ensures that the Bidder's experience is relevant and up-to-date. Projects that have been completed recently or are currently in progress reflect the Bidder's ability to handle similar work in the present context. This criterion acknowledges that ongoing projects can provide valuable insights into the Bidder's current capabilities, expertise, and performance.<br>Demonstrated Capability to Satisfy Customers: The satisfactory letters from customers as on the date of bid submission, who have received services from ongoing projects provides strong evidence of the Bidder's ability to meet customer | For point - 2, refer corrigendum.<br>Rest as per RFP. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 5.4.6 | 14 | Prepration of Bid | The bids submitted by a consortium of companies/firms or any subcontractors will be rejected. | **1.** As per Point No 6.11, Page no 30 , Subcontracting by Data Centre Operator is allowed for both IT and Non IT work. Request to please delete this clause to avoid conflict.<br>**2.** Consortium bidding should be allowed. | | As per RFP |
| 3 | Annexure - B.G | 163 | Next Generation Firewal | The solution should have atleast 4 X 1G/10G Cu, 16 X 10G/25G (SFP/ SFP+), 4 X 40G/100G (QSFP/ QSFP+) with all ports fully loaded from day 1. | **1.** The solution should have atleast 4 X 1G/10G Cu, 16 X 1G/10G (SFP/ SFP+), 2 X 40G/100G (QSFP/ QSFP+) with all ports fully loaded from day 1.<br>**2.** Please clarify if the requirement is of 16 ports of SFP/SFP+ or SFP+/SFP28 because 16 ports of SFP28 is specific to OEM architecture/framework. Please modify the clause as "The solution should have atleast 4 X 100/1000/10G Cu , 16 X 1G/10G SFP/ SFP+ , 4 X 40G/100G QSFP28 with all ports fully loaded from day 1 with defined transceivers type as ****" and even clearly state that whether the bidder/OEM has to provide both SFP and SFO+ transceivers and even 40G &100G transceivers. Also, there should be a mention about whether the transceivers should be SM or MM.<br>**3.** The solution should have atleast 4 X 1G/10G Cu, 16 X 10G/25G (SFP/ SFP+), 2 X 40G/100G (QSFP/ QSFP+) with all ports fully loaded from day 1. | **1.** Our undertsanding here is that ports requirement is 4*1G or 4*10G ports,similarly 16*10G ports or 16*25G ports.Please clarify if our understanding is correct.As 16*25G ports would make us and other leading oems non compliant.Request your clarification here<br>**2.** Request to specify the exact transceiver type to be provided as part of the BOQ from day 1.<br>**3.** Considering the other performance parameters, ports requirements are on higher side. Therefore, request you to reconsider the changes as suggested. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | Annexure - B.G | 164 | Next Generation Firewal | Firewall solution based on upto 3U space design form factor. | To be deleted. | **1.** Restricting scalable solution for Data Center future requirement or restricting Data Center scalability.<br>**2.** Restricting scalable solution for Data Center future requirement or restricting Data Center scalability. | As per RFP |
| 5 | Annexure - B.G | 165 | Next Generation Firewal | Proposed solution will able to provide accurate identification and classification of all devices on a network, including never-before-seen devices. | To be deleted. | **1.** OEM Propeitary Specification.<br>IoT device inspection by the firewall will create an overhead burden on the firewall utilization and may choke the network bandwidth. It is recommended to have a separate virtual IoT devices.<br>Request to reconsider the changes as suggested for wider participation.<br>**2.** OEM Propeitary Specification.<br>IoT device inspection by the firewall will create an overhead burden on the firewall utilization and may choke the network bandwidth. It is recommended to have a separate virtual IoT devices.<br>Request to reconsider the changes as suggested for wider participation. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | Annexure - B.G | 165 | Next Generation Firewal | Proposed Solution must have Iot Device security feature which support ML-based anomaly detection | To be deleted. | **1.** OEM Propeitary Specification.<br>IoT device inspection by the firewall will create an overhead burden on the firewall utilization and may choke the network bandwidth. It is recommended to have a separate virtual IoT devices.<br>Request to reconsider the changes as suggested for wider participation.<br>**2.** OEM Propeitary Specification.<br>IoT device inspection by the firewall will create an overhead burden on the firewall utilization and may choke the network bandwidth. It is recommended to have a separate virtual IoT devices.<br>Request to reconsider the changes as suggested for wider participation. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | Annexure - B.G | 165 | Next Generation Firewal | Should have more than 10,000 (excluding custom signatures) IPS signatures or more. | **1.** Should have more than 10,000 (excluding custom signatures) IPS signatures or more. Should support more than 10,000+ (excluding custom application signatures) distinct application signatures.<br>**2.** Should have more than 20,000 (excluding custom signatures) IPS signatures or more.<br>**3.** Should have more than 10,000 (excluding custom signatures) IPS signatures or more. Should support more than 10,000+ (excluding custom application signatures) distinct application signatures. | **1.** If application signature for specific application not available in firewall then administrator need to use port, link, services to create custom application or services which will open gates to wider application and could lead to an entry to malicious application. More application signatures will strengthen security since pre-defined signatures match the application rule on the basis on signature.<br>Therefore, request you to re-consider the changes as suggested.<br>**2.** Wider signature reference will ensure better security efficacy for the critical SDC infrastructure.<br>**3.** If application signature for specific application not available in firewall then administrator need to use port, link, services to create custom application or services which will open gates to wider application and could lead to an entry to malicious application. More application signatures will strengthen security since pre-defined signatures match the application rule on the basis on signature. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8 | Annexure - B.G | 165 | Next Generation Firewal | The firewall should be supported Third party log analyzer tools and Log server and SIEM /event correlation module for NGFW & Anti APT. | **1.** The firewall should be supported Third party log analyzer tools and Log server and SIEM /event correlation module for NGFW & Anti APT. Firewall and Anti-APT (if procure from same OEM) must be able to manage from same management console.<br>**2.** The firewall should be supported Third party log analyzer tools and Log server and SIEM /event correlation module for NGFW & Anti APT. Firewall and Anti-APT (if procure from same OEM) must be able to manage from same management console. | **1.** Firewall threat prevention policies of zero day attack should be managed from same console and should be implied on APT device which is in line with firewall. Having an additional APT console will not be in sync with firewall and could lead to conflict in firewall and APT policies. Therefore, both APT and firewall should be managed from same management console. Kindly reconsider the changes as suggested.<br>**2.** Firewall threat prevention policies of zero day attack should be managed from same console and should be implied on APT device which is in line with firewall. Having an additional APT console will not be in sync with firewall and could lead to conflict in firewall and APT policies. Therefore, both APT and firewall should be managed from same management console. Kindly reconsider the changes as suggested. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | Annexure - B.G | 166 | Next Generation Firewal | The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. | **1.** The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. Threat Intelligence and IPS signature base must not be from same OEM in Intranet Firewall and Internet firewall considering the defense and depth approach.<br>**2.** The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. Threat Intelligence and IPS signature base must not be from same OEM in Intranet Firewall and Internet firewall considering the defense and depth approach. | **1.** No vendor is immune to security vulnerabilities. By diversifying the OEMs for data center firewalls, we can reduce the likelihood of a single vendor-specific vulnerability compromising both your intranet and internet security.<br>If a vulnerability or weakness is discovered (which has been discovered recently in one of the leading OEM OS) in one firewall, having another firewall from a different OEM reduces the risk of the same vulnerability being present in both devices. Even if one firewall is compromised or has a security flaw, the other firewall can help mitigate the risk and prevent unauthorized access or malicious activities.<br>Therefore, request to reconsider the changes as suggested.<br>**2.** No vendor is immune to security vulnerabilities. By diversifying the OEMs for data center firewalls, we can reduce the likelihood of a single vendor-specific vulnerability compromising both your intranet and internet security.<br>If a vulnerability or weakness is discovered (which has been discovered recently in one of the | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 10 | Annexure - B.G | 166 | Next Generation Firewal | The management platform must be a dedicated OEM appliance for Centralized Management, Logging and Reporting. | **1.** The management platform must be a dedicated OEM appliance for Centralized Management, Logging and Reporting. Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy.<br>**2.** The management platform must be a dedicated OEM appliance for Centralized Management, Logging and Reporting. Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy | **1.** Any traffic reaches to firewall will scan through all the security rules until any rule matches the traffic and if no traffic meet then the traffic drop by deny rule which is resulting in high CPU utilization of resources. Sub-policy structure helps firewall to identify specific rule and reduces the CPU utilization.<br>Sub-policy structure helps in segregating the policies among 10000+ rules to identify or to create additional rules if require.<br>Therefore, reconsider the changes as suggested.<br>**2.** Any traffic reaches to firewall will scan through all the security rules until any rule matches the traffic and if no traffic meet then the traffic drop by deny rule which is resulting in high CPU utilization of resources. Sub-policy structure helps firewall to identify specific rule and reduces the CPU utilization.<br>Sub-policy structure helps in segregating the policies among 10000+ rules to identify or to create additional rules if require.<br>Therefore, reconsider the changes as suggested. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11 | Annexure - B.G | 166 | Next Generation Firewal | The management platform must provide centralized logging and reporting functionality. The management platform must provide a customizable dashboard. | **1.** The management platform must provide centralized logging and reporting functionality. The management platform must provide a customizable dashboard. Must support MITRE ATT&CK view to investigate security issues according to the MITRE defense models, and extract immediate action items based on the mitigation flow.<br>**2.** The management platform must provide centralized logging and reporting functionality. The management platform must provide a customizable dashboard. Must support MITRE ATT&CK view to investigate security issues according to the MITRE defense models, and extract immediate action items based on the mitigation flow | **1.** MITRE framework provides hollistic overview of attack kill chain in one single framework to identify any attack and also helps in forensic. Request you to add the crucial security features.<br>**2.** MITRE framework provides hollistic overview of attack kill chain in one single framework to identify any attack and also helps in forensic. Request you to add the crucial security features. | As per RFP |
| 12 | 7.3.2.5.2 | 39 | Upgradation of PSDC | Application Performance Monitoring & Network Behaviour Analyzer (APM & NBS) | Application Performance Monitoring (APM) | Specifications mentioned in the RFP are of the APM not of NBS. So request you to go for an upgrade with existing NBS solution since the specifications are not in line with the NBS requirement.<br>Request you to reconsider the changes as suggested. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 5.10 | 16 | Technical Bid Evaluation | Average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22<br>▪ Above 400 Crores: 20 Marks<br>▪ >300 Crores & <=400 Crores: 15 Marks<br>▪ >=200 Crores & <=300 Crores: 10 Marks Balance Sheet / Profit & Loss statement / CA Certificate | **1.** Suggest to increase the average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22<br>▪ Above 600 Crores: 20 Marks<br>▪ >400 Crores & <=600 Crores: 15 Marks<br>▪ >=200 Crores & <=400 Crores: 10 Marks<br>**2.** Average annual turnover of bidder in India for any three of last five financial years reported i.e. till FY 2021-22<br>▪ Above 300 Crores: 20 Marks<br>▪ >250 Crores & <=300 Crores: 15 Marks<br>▪ >=200 Crores & <=250 Crores: 10 Marks | **1.** Will help qualify larger SI/ service providers.<br>**2.** The tender qualification criteria currently state that the asked average annual turnover is higher side. By reducing the scoring criteria to encourage maximum participation from potential bidders. Enhancing Competition: By reducing the scoring criteria, more bidders will be able to meet the qualification requirements and participate in the tender process. This increase in competition benefits the organization as it promotes a broader pool of potential vendors, resulting in improved quality, competitive pricing, and innovative solutions. A larger participation base ensures a more comprehensive evaluation of available options, ultimately leading to better value for the organization. | As per RFP |
| 14 | 5.1 | 11 | Eligibility / pre-qualification criteria | Bidders are required to submit bid specific Manufacturing Authorization Form (MAF) confirming that the products quoted are neither end of sale nor end of life. For the OEM's of all IT & non-IT assets to be provided by the bidder. | We request you for amendment MAF for Non-IT some specific major Non-IT products only and MAF should not required for all Non-IT products otherwise small Non-IT vendor will manage the bid. | Otherwise smal Non-It products OEMs/vendor will manage the bid and due to this eligible bidders will restrict to bid. | Refer Corrigendum |
| 15 | 3.E | 203 | UPS Critical Load | Same shall be compliant to OSHA, IEC and certified by UL (Underwriters Laboratory) | The UPS is complied to IEC standards. UL standard are not complied | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 3.H | 203 | UPS Critical Load | Life cycle monitoring of critical components such as AC/DC Capacitors, Battery bank, cooling fans. | Only battery life cycle prediction will be available | | As per RFP |
| 17 | 3.K.e | 204 | UPS Critical Load | Maintenance bypass: In maintenance bypass the load is supplied with unconditioned power from the manual maintenance bypass input switch provided in a separate enclosure with each UPS. | Generally manual bypass for more than 2 UPS in parallel is located in output panel, please confirm whether inbuilt manual bypass is required or it is designed in output panel of UPS | | For parallel configuration, external wrap around bypass is required. |
| 18 | 3.K.f | 204 | UPS Critical Load | Static Bypass operation with Power Factor Improvement & Harmonic Mitigation: UPS shall be capable to mitigate Harmonics (THDI) to < 5% and Power Factor Improvement to 0.99 at full load while UPS is operating in Static Bypass in<br>Economy mode. The UPS vendor may supply an active harmonic filter in UPS bypass path if this is not a standard feature available in the UPS. The overall condition in bypass operation in Economy mode. | THDi & PF correction are maintained in online double conversion mode. As DC load is critical it is not recommended to run the UPS continuously on bypass, hence THDi & PF correction is not available in ECO mode | | As per RFP |
| 19 | 3.R.g | 205 | UPS Critical Load | Short Circuit Handling Capability of the Inverter: 250% of nominal current for 5000 milliseconds. | As per industry standards, this is generally 250% for 100 msec | | As per RFP |
| 20 | 3.R.j | 205 | UPS Critical Load | System Efficiency: Greater than equal to 96% at 25% loading , >97% on 50% to 100% loading conditions | Generally Efficiency is >96% from 25% to 100% loads. | | As per RFP |
| 21 | 3.S.vi | 206 | UPS Critical Load | Forced Air Cooling: Redundant cooling fans shall be provided in each sub-module of the UPS so that one fan failure in each sub-module of the UPS does not result into degraded operation of the UPS. | Generally fan redundancy is available on 25 degree temperature | | As per RFP |
| 22 | 3.S.viii | 206 | UPS Critical Load | Built In / External Energy Meter shall be provided to display kWh consumption at input & output. | Generally kWH meter is at input only. | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 23 | | 209 | Features of Monitor Panel for Indications, Diagnostics and Control | Display Parameters: Output Voltage / current/ frequency (RMS value &Peak value) | As per industry standards, only RMS values are displayed on UPS display | | As per RFP |
| 24 | | 212 | Features of Monitor Panel for Indications, Diagnostics and Control | Battery Type: Li-Ion (Make : Samsung/LG) | We request to consider Delta make NMC type Lithium Ion batteries | | Accepted provided it should be compliant with UL9540A certification |
| 25 | | | General Query | | What all are the databases hosted in data centre(Sql & NoSql) | | My-SQL, ORACLE, Postgres and MongoDB |
| 26 | | | General Query | | What is the deployment topology of these databases | | Standalone, Active Passive and always available on |
| 27 | | | General Query | | Requirement of HA for databases | | Depend on project requirement |
| 28 | | | General Query | | What is the mode of connectivity to DC by the users ? | | SSL VPN |
| 29 | | | General Query | | Please share details of exisitng Licenses which is being used and has to be upgraded ? | | Bidder is only responsible for the licenses which are part of the solution it is to provide as per the scope of tender. |
| 30 | | | General Query | | Is it under service provider's scope to provide various software licenses like OS, DB, middleware etc.? If yes, please share the details with version & editions. | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 31 | | | General Query | | Please provide more details on the Managed Services currently present in the environment. What are the expectations from Bidder ? | | The bidder should be responsible for managing the infrastructure, operating systems, network, security, monitoring, backup, and day-to-day operations related to the hosted department hardware. This comprehensive responsibility ensures that the bidder takes charge of all aspects of the hosted environment to ensure its smooth functioning and efficiency. |
| 32 | | 32 | | | PSDC existing architecture shared in the RFP is a high level architecture, requesting to share detailed Physical & logical diagram of DC? | | Refer clause - 7.1.2 |
| 33 | | | | | As is it mentioned in RFP, good amount of devices could be out of support or maybe not running up to mark firmware. In this scenario we will need existing Service provider to provide us up to date devices with support contract details & update firmware version? | | Refer to Annexure - A |
| 34 | 7.1.3.2 | 32 | | | It is mentioned that the selected bidder shall undertake the design, supply, build, installation, and commissioning of new IT. We would like to understand how the cost estimation will happen, is it the 1st party who will provide us the cost approval? The question is mainly how we will do the hardware cost estimation? | | Bidder to quote the cost in commercial sheet as per it's solution. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 35 | 7.1.3.1 | 32 | | | The survey report is to be submitted within 1 month from the signing of the contract.-- can this be extended to 2 months ? | | As per RFP |
| 36 | 7.2.3.4 | 34 | Data Privacy & Security | | What is the scope of data privacy in the context of physical data centre | | "Data Privacy & Security" mentioned at clause - 7.2.3.4 is not related to physical security. But DC Floor physical security is also under the Bidder's scope. |
| 37 | 7.3.2.5.5 | 40 | Endpoint Security | | **1.** What is the BOQ, Existing Architecture of endpoint security (TrendMicro) and Scope of managed services. **2.** Which method of service is acceptable to the department? Cloud based or Client-Server on premise model, please clarify | | The existing architecture for endpoint security includes TrendMicro and Symantec, which are managed by DCO (Data Centre Operations). In order to prioritize data centre security, a client-server on-premise model will be preferred. |
| 38 | 7.3.2.5.4 | 40 | Next Generation Firewall (NGFW) | | What is the security log retention period and storage to be considered? Is there any other security building blocks has to be considered in the solution? | | 6 month's offline and 3 month's online |
| 39 | 7.4.4.1 | 43 | Operation and Management of PSDC | System / Network / Storage / Security / Application / Backup / Physical infrastructure Administration, Monitoring, Maintenance & Management Services. | Need clarity on the Scope of managed security services for IT landscape. Will the bidder be responsibe for managed security services for IT enviroment for hosted Data center of the tenants hosting their infra/services in the state data center. | | The bidder is responsible for providing administration, monitoring, maintenance, and management services for the system, network, storage, security, applications, backup, and physical infrastructure. Additionally, the bidder is expected to offer security support for co-location services. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 7.4.13.9 | 46 | PSDC website | This website shall adhere to all latest security compliances along with GIGW compliances issued by MietY and CERT-IN | Is Web App Scan a part of the bidder scope? | | As per RFP |
| 41 | 7.4.15.1.7 | 48 | System Administration, Maintenance & Management Services | Necessary action shall be taken by the service provider in accordance with the results of the log analysis. Suitable mechanism has to be maintained for the Information Security Management System (ISMS) by the service provider following forensic or other governmental regulations from time to time. Service provider to refer CERT-In guidelines available for the State Data Centre. Service<br>providers have to coordinate and provide all the support for such requirements during the entire project tenure | What is to be the retention period of the logs?<br>Are the logs to be queried? If yes, what will be the frequency of the querying?<br>Are the logs only to be stored or to be used for incident analysis? | | Refer clause - 7.4.15.1 |
| 42 | 7.4.17 | 50 | Security Incident & Event Management | | Is there a feasibility to opt cloud based SIEM solution ? | | No |
| 43 | c.f | 88 | Non IT Assets | Security and Incident Management SLA's | For every virus attack reported, Any other security related threat, For every incidence of Denial of service attack - Legal view sought here - as here every INCIDENT is penalised, as against critical/ service impacting incidents/threats. | | As per RFP |
| 44 | | 89 | Security and Incident Management SLA's | Liquidated damages applicable per month against the following incidents | the word "incident" should be changed to "impacting incident", Legal view sought here | | As per RFP |
| 45 | 7.3.2.5.3 | 40 | Enterprise Management System (EMS) | Currently, PSDC is using CA spectrum which helps for infra / network / services monitoring | Is DGRPG open to evaluate SaaS solution as an EMS ? | | No, as per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 46 | Annexure - B.D | 157 | Helpdesk and IT Service Management | Helpdesk" shall mean the 24x7x365 support center which shall handle fault reporting, trouble ticketing and related enquiries during this contract. | Is this dedicated or Shared HelpDesk? Onsite or Remote? Can we use existing Helpdesk tool including helpline number etc? | | Dedicated onsite heldpdesk is required. Further, refer clause - 7.4.31.2. |
| 47 | Annexure - B.D | 157 | Helpdesk and IT Service Management | Helpdesk" shall mean the 24x7x365 support center which shall handle fault reporting, trouble ticketing and related enquiries during this contract. | Please share previous 6 months ticket volume and trends? | | Scope of current DCO is limited and current ticket volume will not represent the true picture. |
| 48 | Annexure - B | 153 | EMS/NMS Specifications for 05 Years warranty and AMC support: | Proposed solution should have Out-of-the-Box connectors/ probes/ Rest API's to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS | Can we have any relaxitation on this clause ? | | As per RFP |
| 49 | 4.1.2 | 9 | The Data Centre was commissioned in Oct., 2017 | The Data Centre was commissioned in Oct., 2017 | Please share details of existing infra and their intsalltion date and expiry | We need details to assess equipment aging, performance as well as to have costing of hardware components to be procured and design documents will be required to check feasibility of components to be used in Tier III DC with existing infra | Refer Annexure - A |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 50 | 7.1.3.2 | 32 | Upgradation of the PSDC | Upgradation of the PSDC-The selected bidder shall undertake design, supply, build, installation and commissioning of new IT & Non-IT infra.This includes, but may not be limited to, firewall upgradation, enhancing Building Management System, better structuring of cables, Fiber runner, reporting & logging software, online helpdesk, hosting request & invoice system. Load capacity per rack is to be increased from 4 KVA to at least 10 KVA. Refer section – 7.3.2 for details. DCO shall offer the site for Final Acceptance Testing (FAT). | Load Capacity per rack increament from 4 KVA to 10 KVA is to be done in colaboration with DGRPG Punjab & Bidder | Required approval from electrcity board/ Authorities is to be taken by DGRPG Punjab | This is internal upgradation of PSDC racks. Bidder to proceed as per scope. |
| 51 | 7.2.3.1 | 33 | Process, Policies & Guidelines | Process, Policies & Guidelines | Requesting to define the process, policies & guidelines to be followed while managing SDC | We need further more details on Process and Policies to be followed in order to meet DGRPG expectations. | To be taken from existing DCO as part of HOTO. |
| 52 | 7.2.4 | 34 | status of software's (like; license expired, license expiry date, license valid till date etc | status of software's (like; license expired, license expiry date, license valid till date etc | Kindly share details of exisiting Hardware/Software expriy details | It will be helful for us to understand and listdown IT/NonIT equipments to be procured and maintain DC for Site survey | Refer Annexure - A |
| 53 | 7.3.1.6 | 36 | Service Provider shall install hot and cold aisles in the server farm area. | Service Provider shall install hot and cold aisles in the server farm area. | Please share details of existing Hot&Cold Aisles | Would be helpful to identify compents required during upgradation to Tier III DC | Hot & Cold containment is not available with existing DCO. Rows with cold air intakes – the fronts of servers – facing each other (the "cold section") and hot air exhausts – the backs of servers – facing each other (the "hot section"). |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 54 | 7.4.44.1 | 68 | The Data Centre operator shall be responsible for Electricity and Diesel Management for the entire project period. The Data Centre Operator shall ensure that diesel shall be there in the DG sets all the time to maintain the SLA and ensure no downtime of SDC. | The Data Centre operator shall be responsible for Electricity and Diesel Management for the entire project period. The Data Centre Operator shall ensure that diesel shall be there in the DG sets all the time to maintain the SLA and ensure no downtime of SDC. | Kindly share details of current consumption pattern and expected consumption after upgradation ? Is there any limitation/ restriction of usage on DG | We need to assess expected consumption and request for Maximum Demand enhancement from state electricity board | The current fuel consumption as per the load for the DG set is approximately 45 to 60 liters per hour per DG set. |
| 55 | | 122 | Annexure - A-Non-IT-Diesel storage | Annexure - A-Non-IT-Diesel storage | Please specify Diesel storage capacity for backup | To understand whether storage to be upgraded or not ! | The PSDC DG Set has a diesel tank capacity of 990 L x 3, totaling 2970 L. |
| 56 | | 122 | Annexure - A-Non-IT- Provision of Diesel | Annexure - A-Non-IT- Provision of Diesel | Kindly define whose responsibility is to procure Diesel and trasport to the DC location | Information is required to define roles and responsibilites | Its responsibility of DCO. |
| 57 | | 122 | Annexure - A-Non-IT | Annexure - A-Non-IT | Kindly share Rack PDU details : Configuration with BMS system | During upgradation details will be required | Refer to table "List of Existing Electrical Assets in PSDC" in Annexure - A. |
| 58 | | 122 | Annexure - A-Non-IT | Annexure - A-Non-IT | Kindly share fire suppression details | Detail required for costing | Refer to table "List of Existing Fire Suppression Assets in PSDC" and "Fire & safety Assets in PSDC" in Annexure - A. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 59 | 5.10 | 17 | Technical bids evaluation | No. of certified Data Centers managed by the bidder in last 10 years: -<br>4 Marks for each Uptime Tier-II or TIA-942 Rated 2 Data Centre<br>OR<br>10 Marks for each Uptime Tier-III or TIA-942 Rated 3 Data Centre<br>OR<br>20 Marks for each Uptime Tier-IV or TIA-942 Rated 4 Data Centre | **1.** No. of certified Data Centers managed by the bidder in last 10 years: -<br>10 Marks for each Uptime Tier-II or TIA-942 Rated 2 Data Centre<br>OR<br>20 Marks for each Uptime Tier-III or TIA-942 Rated 3 Data Centre<br>**2.** No. of certified Data Centers managed by the bidder/Consortium Partner/Sub-contractor in last 10 years: -<br>4 Marks for each Uptime Tier-II or TIA-942 Rated 2 Data Centre<br>OR<br>10 Marks for each Uptime Tier-III or TIA-942 Rated 3 Data Centre<br>OR<br>20 Marks for each Uptime Tier-IV or TIA-942 Rated 4 Data Centre.<br>**3.** No. of certified Data Centers managed by the<br>bidder in last 10 years: -<br><br>1 to 2 Data centres: 10 Marks<br>3 to 4 data centres: 15 Marks<br>More than 4 data centres: 20 Marks | **1.** Consortium allows stakeholders to leverage their combined resources, and industry expertise, to reach a wider audience and achieve more significant results. Also consortium experience allows either partner to support each other in case of fianancial crisis of lead member and make sure all deliverables towards end customers are ensured.<br><br>Hence, we request to please allow consortium or sub-contractor experience experience like in other similar projects in Punjab as well other states in India as under"<br>1.Punjab State E-Governance RFP No. PSEGS/SEWA KENDRAS/2018/Z1<br>PUNJAB STATE e-GOVERNANCE SOCIETY<br>Department of Governance Reforms<br><br>2. State Data Center RFP No. CC/NT/W-CIVIL/DOM/A06/23/00358<br>Power Grid Corporation of India | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 60 | Annexure - B.G | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have at least 2TB log capability internally along with support for scalable external storage (eg: SAN/RAID) feature | **1.** Solution should have at least 8TB log capability with dedicated log appliance.<br>**2.** Firewall Solution should have at least 2TB log capability along with support for scalable external storage (eg: SAN/RAID) feature | **1.** Restrictive Point: Every OEM has its own set of architecture and point is favouing single OEM. So we suggest you to please make it generic and ask the reports on separate appliance with higher harddisk. We don't recommend to keep the logs and report on the firewall. Considering the datacenter environment the asked harddisk is very less.<br>**2.** RFP has already asked for dedicated centralized managmement platform for logging, reporting . Hence request to change the caluse "Firewall Solution should have at least 2TB log capability along with support for scalable external storage (eg: SAN/RAID) feature" | Refer Corrigendum |
| 61 | Annexure - B.G | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have inbuilt redundant hot-swappable power supply and in built hot-swappable/replaceable fans/ tray/ modules | Firewall Solution should have inbuilt redundant hot-swappable power supply and /swappable Fans/redundant fans/ tray/ modules | Restrictive Point:<br>Every OEM has its own set of architecture and we offer redundant hotswappable Power supply. But for fans we have fixed architecture. So request you to please ammend the point. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 62 | Annexure - B.E | 160 | Security Incident Management Solution (SIEM) | The solution should be able to collect the logs in an agent/ agentless manner and store the same in real-time to a Central log database from any IP Device. The logs should be time stamped, compressed to optimize storage utilization. There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department. | The solution should be able to collect the logs in an agent/ agentless manner and store the same in real-time to a Central log database from any IP Device. The logs should be time stamped, compressed to optimize storage utilization. | Restrictive Point:<br>Every OEM has its own set of architecture and licensing model. So we recommend you to share the total no of device count from day one with future expansion scope so that we can factor the device count accordingly. Please consider the point so that we can take part and give tough competition to the competitor and price benefit to the organization. You can also refer multiple RFP in the region where they have mentioned device count from dayone. | As per RFP |
| 63 | 5.6.1 | 14 | Validity of bids | Bids shall remain valid till 90 days from the date of submission of bids. DGRPG reserves the right to reject a proposal valid for a shorter period as non-responsive. | We request that the clause be modified as follows:<br>Bids shall remain valid till 60 (sixty) days from the date of submission of bids. DGRPG reserves the right to reject a proposal valid for a shorter period as non-responsive. | The prices quoted for the products and services are dynamic in nature which will keep changing in short periods of time. Due to this, 90 days' period is quite long and hence the request for reduction of the validity to 60 days. | As per RFP |
| 64 | 5.14.1 | 21 | Performance security | As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish performance security @10% of the contract value to DGRPG as performance security. | We request that the clause be modified as follows:<br>As soon as possible, but not more than 20 days after the issue of Letter of Intent (LoI), the successful bidder shall furnish performance security @3% of the contract value to DGRPG as performance security. | The value of the PBG at 10% is quite high considering the nature of the tender. PBG of 3% is commensurate with the tender and hence we have requested for reduction of the PBG amount. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 65 | 5.14.2 | 21 | Performance security | After FAT, the Service Provider shall furnish performance security @5% of the contract value to DGRPG which shall remain valid for a period of 180 days beyond the expiry of the contract. The previous PBG submitted by the Service Provider as per clause 5.14.1 would be returned back. | We request that the clause be modified as follows:<br>PBG shall remain valid for the period of the contract. Whenever the contract is extended, Service Provider will have to extend the validity of PBG proportionately. | The PBG is obtained by the customer for ensuring performance of the contract by the bidder. Therefore, the PBG should expire at the time of expiry of the contract and not beyond such expiry. | As per RFP |
| 66 | 6.11.2 | 30 | Subcontracting by Data Centre Operator | It is clarified that the service provider shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the subcontractors, and shall, notwithstanding such sub-contract (or any approval thereof by the Authority) continue to be liable for any work or services provided by any subcontractors. The service provider undertakes to indemnify the Authority from any claims on the grounds stated hereinabove. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the sub-contractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services. | We request that the clause be modified as follows:<br>for any of the work to be carried out by the sub- contractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services. The service provider undertakes to defend and settle any claims on the grounds stated hereinabove with prompt notification and cooperation by the Authortity with the bidder having sole contol of such defence. The service provider shall not allow a sub-contractor to assign or enter into further secondary subcontract for any of the work to be carried out by the sub-contractor. For avoidance of doubt, service provider shall not be allowed to sub-contract the entire Project/work/Services. | In the event that there is a claim from a sub-contractor or sub-contractor employees, then the bidder should be allowed to defend and settle such claims without having to indemnify the authority. Such defence shall be undertaken with prompt notification and cooperation by the authority. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 67 | 6.12.1 | 31 | Insurance | The bidder shall provide comprehensive insurance coverage for all scope assets against any and all types of incidents, including but not limited to fire, theft, riots, earthquake, accidental fire suppression system release, and cyber-attacks, for the entire duration of the project. The insurance coverage shall be in compliance with all relevant Indian laws and regulations and shall include coverage for any damages or losses incurred by the client or any third parties due to the bidder's actions or inactions. The bidder shall provide proof of insurance coverage and maintain it throughout the project duration. | We request that the clause be modified as follows:<br>The bidder shall provide comprehensive insurance coverage for all scope assets against any and all types of incidents, including but not limited to fire, theft, riots, earthquake, accidental fire suppression system release, and cyber-attacks, till the time of installation. The insurance coverage shall be in compliance with all relevant Indian laws and regulations and shall include coverage for any damages or losses incurred by the client or any third parties due to the bidder's actions or inactions. The bidder shall provide proof of insurance coverage and maintain it throughout the project duration. | The bidder's obligation to insure the products and services supplied should be upto the time of installation of the products and not beyond considering the ownership and risk would transfer to the DGPRG. Upon installation, DGPRG should be responsible for obtaining insurance. | As per RFP |
| 68 | | | Limitation of Liability | New clause | We request that the following clause be added as a new clause to the contract for the purposes of limiting the liability of the bidder:<br>To the full extent permitted by law, the Service Provider shall not be liable to DGPRG in respect of any Claim for loss of profits, business, revenue, anticipated savings, goodwill, data or contracts or any type of special, indirect, economic, punitive or consequential loss (including loss or damage suffered as a result of any claims brought by a third party) even if such loss was reasonably foreseeable or the Service Provider had been advised of the possibility of the Service Provider incurring the same. | We request that any indirect or consequential damges should be excluded considering the same would not be foreseeable by the service provider. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 69 | 9.2 | 79 | Project Implementation and Payment Schedule | Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. | We request that the clause be modified as follows:<br>Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. All payments to the bidder shall be made within 30 days from the date of invoice. | The RFP does not provide for a timeline by when the payments will be made. There has to be a specific timeline for payments and hence this change. | As per RFP |
| 70 | 10 | 81 | SLA and Liquidated Damages | SLA and Liquidated Damages | We request that the following clause be added as a generic clause :<br>Liquidated damages or penalties under the contract shall be subject to a maximum cap of 3% of the delayed portion of supply or services | Liquidated damages and penalties should be commensurate with the scope of work and type of work of the bidder. Hence, there has to be a maximum cap of 3% of the delayed services as LDs and penalties are levied only if services are delayed and should accordingly be levied to the extent of delayed supply or services. | As per RFP |
| 71 | 11.1.1 | 93 | Payment Terms | Payment to the Service Provider shall be made in Indian Rupees through NEFT / RTGS only on quarterly basis. | We request that the clause be modified as follows:<br>Payment to the Service Provider shall be made in Indian Rupees through NEFT / RTGS only on quarterly basis. All payments to the bidder shall be made within 30 days from the date of invoice. | The RFP does not provide for a timeline by when the payments will be made. There has to be a specific timeline for payments and hence this change. | As per RFP |
| 72 | 11.1.8 | 94 | Payment Terms | Payments shall be subject to deductions of any amount for which Service Provider is liable under the contract. | We request that the clause be replaced with the following clause:<br>Any liquidated damages or penalties levied on the bidder shall be recovered from the bidder after completion of the contract. | Any deductions from the payments to the contractor shall lead to cash flow and revenue recognition issues and hence should be recovered after completion of the contract. | As per RFP |
| 73 | 5.6 | 14 | 5.6 | Bids shall remain valid till 90 days from the date of submission of bids. | Bidder request to amend bid validity to 60 days | Considering the FX fluctuation and current market volatility | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 74 | 9 | 78 | 9 | Operation and Maintenance of SDC before FAT:<br>50% of the price quoted for O&M before FAT in the Financial bid per quarter (In case of delay in FAT, the O&M cost will be paid on proportional basis for the delay period subject to SLA) | Bidder request to pay the O&M cost before FAT, monthly in arrears | As this work involve manpower salary is paid to the resources monthly in arrears. | As per RFP |
| 75 | 9 | 78 | 9 | Operation and Maintenance of SDC after FAT<br>5% of the price quoted for Opex Cost for PSDC after FAT in the Financial bid per quarter | Bidder request to pay the O&M after FAT monthly In arrears | Resources are paid monthly in arrears | As per RFP |
| 76 | | | | Payment Term is missing | Bidder request to release the payment within 30 days of invoice date | | As per RFP |
| 77 | 10 | 81 | 10 | SLA and Liquidated Damages: | There are multiple liquidated damages defined in RFP, bidder request to cap the the LD penalty at 5% for delayed portion only. 5% cap should include General clause, HOTO and SLA for SDC upgradation | | As per RFP |
| 78 | 10.7 | 82 | SLA for O&M of PSDC | SLA for O&M of PSDC | There are multiple SLA defined and it is capped at 20% of the O&M value, bidder request to cap the SLA penalty of O&M to 10% | | As per RFP |
| 79 | 9.5 | 79 | Project Implementation and Payment Schedule | If any additional hardware (IT/Non-IT) is added / procured for PSDC by DGRPG through any other vendor or is purchased by other user departments for colocation, Service Provider shall provide Operation and Maintenance services for such infrastructure at no additional cost. SLAs shall also be applicable on the service provider as specified under sub-section 10 | Bidder request to remove this clause | Bidder will not be able to bear the SLA for the product/services provided by any other vendor. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 80 | TQ 2 | 17 | TQ 2 | Successful completion of “similar work” (minimum 10 racks) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023.<br>5 marks for each project subject to a maximum of 20 marks. | **1.** Suggest to increase the minimum treshold to 20 Racks<br>**2.** Successful completion of “similar work” (minimum 10 racks) by Bidder/Consortium Partner/ Sub-Contractor in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023.<br>5 marks for each project subject to a maximum of 20 marks.<br>**3.** Successful completion of “similar work”<br>in government (departments/ boards/ corporations/ PSUs/Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023.<br>5 marks for each project subject to a maximum of 20 marks.<br>“Similar Work” means Setup / Operation & Management of Data Centers Projects | **1.** Will help qualify larger SI/ service providers<br>**2.** Consortium allows stakeholders to leverage their combined resources, and industry expertise, to reach a wider audience and achieve more significant results. Also consortium experience allows either partner to support each other in case of fianancial crisis of lead member and make sure all deliverables towards end customers are ensured.<br>Hence, we request to please allow consortium or sub-contractor experience experience like in other similar projects in Punjab as well other states in India as under"<br>1.Punjab State E-Governance RFP No. PSEGS/SEWA KENDRAS/2018/Z1<br>PUNJAB STATE e-GOVERNANCE SOCIETY<br>Department of Governance Reforms<br>2. State Data Center RFP No. CC/NT/W-CIVIL/DOM/A06/23/00358<br>Power Grid Corporation of India | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 81 | TQ3 | 17 | TQ3 | Largest 'Similar Work' executed by the bidder in terms of racks/value.<br>▪ 36 Racks and above: 20 Marks<br>▪ 24 to 35 Racks: 14 Marks<br>▪ 12 to 23 Racks: 7 Marks<br>OR<br>▪ >=50 cr.: 20 Marks<br>▪ >=40 cr. to <50 cr.: 14 Marks<br>▪ >=30 cr. to <40 cr.: 7 Mark | **1.** Request to change the qualification as below:<br>Largest 'Similar Work' for Tier 3 Data Center executed by the bidder in terms of racks/value.<br>▪ 36 Racks and above: 20 Marks<br>▪ 24 to 35 Racks: 14 Marks<br>▪ 12 to 23 Racks: 7 Marks<br>OR<br>▪ >=50 cr.: 20 Marks<br>▪ >=40 cr. to <50 cr.: 14 Marks<br>▪ >=30 cr. to <40 cr.: 7 Marks<br>**2.** Largest 'Similar Work' executed by the bidder/Consortium Partner/ Sub-Contractor in terms of racks/value.<br>▪ 36 Racks and above: 20 Marks<br>▪ 24 to 35 Racks: 14 Marks<br>▪ 12 to 23 Racks: 7 Marks<br>OR<br>▪ >=50 cr.: 20 Marks<br>▪ >=40 cr. to <50 cr.: 14 Marks<br>▪ >=30 cr. to <40 cr.: 7 Marks | **1.** As Punjab DCO is going in for Tier 3 certification it is imperative that the selected service provider/SI must have the experience in building/managing a Tier 3 DC.<br>**2.** Consortium allows stakeholders to leverage their combined resources, and industry expertise, to reach a wider audience and achieve more significant results. Also consortium experience allows either partner to support each other in case of fianancial crisis of lead member and make sure all deliverables towards end customers are ensured.<br>Hence, we request to please allow consortium or sub-contractor experience experience like in other similar projects in Punjab as well other states in India as under"<br>1.Punjab State E-Governance RFP No. PSEGS/SEWA KENDRAS/2018/Z1<br>PUNJAB STATE e-GOVERNANCE SOCIETY<br>Department of Governance Reforms<br>2. State Data Center RFP No. CC/NT/W-CIVIL/DOM/A06/23/00358 | As per RFP |
| 82 | 7.3.1.4 | 36 | Design of the Data Centre | Heavy equipment, if any proposed, shall be placed keeping in view the floor strengthening. Floor strengthening and any kind of waterproofing shall be in the scope of the selected bidder | Suggested to share existing capacity of floor with composition details to design new floor design. Since in production environment the floor strengthening will be challenge. It should be purely on the basis of equipment placement, selection and design approach of bidder. | Revision of floor strengthening is subject to details available on existing strength of the floor OR Design criteria of floor. | Bidder may visit the data center for the same. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 83 | 7.3.3.2.3 | 42 | Final Acceptance Testing | All documents related to PSDC upgradation and relevant acceptance test (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the DGRPG. | Suggested to keep 2 FAT, one non-IT other IT | Since the non IT part will be ready well in advance than IT final testing, same comes in different set of testing methodology for acceptance. | As per RFP |
| 84 | 7.5.1(10) | 70 | Roles and Responsibility | Obtain Electrical & Fire NOC from concerned Departments. DGRPG will assist for the same. | Existing Fire and Electrical approvals to be provided by DGRPG. DCO shall obtain only the extended part of Fire NOC than full premises/facility. | Permission from builders for upgradation/replacement, changes if any on electrical, DG, Panels on ground floor and basements if any must be provided by DGRPG in time bound schedule. Approvals is required in writing for procurement and site installation testing and commissioning. | Refer Corrigendum |
| 85 | 7.5.1(12) | 70 | Roles and Responsibility | Physical Security of SDC | Clear scope request - IS IT pertains to providing security guards an manpower ? | Clear scope is requested | Refer clause - 7.4.18 |
| 86 | 7.5.1(24) | 72 | Roles and Responsibility | Recurring expenditure like electricity, diesel, after implementation during the Operation and Maintenance Phase | Supply of Diesel and electricity to remove from DCO scope | Fuel supply / Electricity bill: directly procured by DGRPG. DCO will help in management on site with documentation, handling | Refer Corrigendum |
| 87 | 7.5.1(25) | 72 | Roles and Responsibility | Obtain regulatory and other clearances for setting up the extended Data Centre | Facility occupied by DGRPG, since DCO's scope and responsibility not comes in scenario. | The same is applicable in Green field datacenter facility construction start. Hence the scope matrix is requested to change. | Refer Corrigendum |
| 88 | 9.1,2 | 78 | Project Implementation and Payment Schedule | 50% of the price quoted for O&M before FAT in the Financial bid per quarter (In case of delay in FAT, the O&M cost will be paid on proportional basis for the delay period subject to SLA) at T9 - | 25% at T3 completion of HOTO, and 50% on T9 - completion of FAT | Since the HOTO Start, manpower cost is started, billing and revenue cycle for payments at T9 will be much delayed. Advance service tax hit to DCO in case of delayed payment | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 89 | 9.2 | 79 | Project Implementation and Payment Schedule | Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. | Clear scope of criteria requested at time of Bid closure. | Corresponding Financial Risk assessment to be taken in consideration due to non clear criteria of Scope for payment clearance. | As per RFP |
| 90 | 9.8 | 79 | Project Implementation and Payment Schedule | Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. | Request to keep all extra items as Change request OR Non tender items on separate price submission basis | Estimation is non linear in case of open ended scope or item requirement in project | As per RFP |
| 91 | 9.9 | 80 | 9.9 | All payments shall be made corresponding to the goods or services delivered, installed, or operationally accepted, per the Contract Implementation Plan, at unit prices and in the currencies specified in the Financial Bid | Payment milestone criteria to supersede the clause | Request clause merger | Refer Corrigendum |
| 92 | 7.6 | 73 | Manpower & required Resources | 7.6.2 Apart from SPOC, DCO shall deploy suitable IT and non IT manpower to maintain & manage all the operations (including IT, Non IT, Security, Helpdesk, back office etc.) of PSDC so as to maintain the Service Level Agreements. | Is the bidder allowed to use partner model for providing the resources with scope based delivery owned by bidder. | This would the bidder more versitality in proposing most optimal solution. | Refer clause no.: 6.11 - Subcontracting by Data Center Operator |
| 93 | 9.2 | 79 | Project Implementation and Payment Schedule | Payments will be made subject to verification and clearance from the Third Party Agency (TPA) as and when appointed. | What kind of TPA verification if any will be required during Operations and Maintenance phase. | Planning in advance to ensure that the cash flows are maintained in regular and timely manner. | All the payments to be made to service provider after submission of reports by TPA for opex invoices /capex invoices and security audit. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 94 | 9.5 | 79 | Project Implementation and Payment Schedule | If any additional hardware (IT/Non-IT) is added / procured for PSDC by DGRPG through any other vendor or is purchased by other user departments for co- location, Service Provider shall provide Operation and Maintenance services for such infrastructure at no additional cost. Service Provider shall not be responsible for provision of AMC of such infrastructure but vendor management, if any required, shall be the responsibility of the Service Provider. SLAs shall also be applicable on the service provider as specified under sub-section 10. Service Providers may deploy extra manpower to carry out the responsibilities to meet this requirement at no additional cost to the DGRPG. | Additional hardware will need additional efforts for managing and may need additional manpower and maybe with different skill set as well. So this should be through change management. | Anticipating subject purchases and commiting support for it is not possible at this stage and hence it is requested that the same be done at that time with propoer change management process. | DCO will be informed in advance and DCO must have offsite capabilty in case required. |
| 95 | | 92 | Project Implementation and Payment Schedule | Maximum amount of liquidated damages shall be 20% of opex cost | This penalty should be capped @5% of quarterly value. | | As per RFP |
| 96 | | | | General | Please share the Call details volume for last 6 months | It is required to analyse and assess the trend and work on optimal solution appropriately. | Scope of current DCO is limited and current ticket volume will not represent the true picture. |
| 97 | 7.3.2.5.2 | 39 | | Application Performance Monitoring & Network Behaviour Analyzer (APM & NBS): Currently, PSDC is using the Network Behaviour Analyzer solution of Checkpoint | **1.** Please clarify, if existing product is to be upgraded or any other OEM would be acceptable.<br>**2.** Please clarify, if existing product is to be upgraded or any other OEM would be acceptable | | Existing solution upgradation with same OEM or different OEM will be accepted but tender specifications have to be fulfilled. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 98 | 7.3.2.5.3 | 40 | | Enterprise Management System (EMS)<br><br>Proposed solution should support following: -<br>i. Asset Management<br>ii. Monitor the availability of Services<br>iii. Fault Management<br>iv. Performance Management (Server, Network, Security, SAN etc)<br>v. Security information management (analyze logs of servers, network devices) | Does the existing product CA spectrum has these features? Will any other OEM be acceptable with all these features? | | These features are considered as the basic requirements. However, if any Original Equipment Manufacturer (OEM) offers additional or advanced features, they will be considered and accepted. |
| 99 | 7.3.2.5.4 | 40 | | Next Generation Firewall (NGFW) - PSDC is using Checkpoint 12200 firewall in HA mode and is required to be upgraded with following configurations:- 8 x 10/100/1000Base-T RJ45 ports, One network card expansion slot, 8 GB memory, 2 x 500 GB HDD, LOM card, Slide rails (22" to 32"), 1.7 (default)/5(max) million concurrent connections, 90,000 connections per second.Proposed solution should be a multicore CPU architecture with a hardened 64-bit operating system and should be support Third party log analyzer tools / Log server/ Siem/event correlation module for NGFW & AntiAPT. Solution Should provide Min 20 Gbps Threat Protection Throughput (NGFW + AVC + IPS + Antivirus + Antibot/Anti Spyware/Anti Malware + Zero Day) with logging enabled and tested with Enterprise Mix/Production raffic/Real World Traffic. | **1.** Are these specifications of existing firewall? Please clarify.<br>**2.** Are these specifications of existing firewall? Please clarify.<br>**3.** Please provide clarification regarding the disparity between the firewall configuration mentioned in clause 7.3.2.5.4 on page 40 and the one on page 163. Kindly specify which current firewall should be replaced with the given configuration. Additionally, I request the removal of the LOM card restriction, as it is applicable only to a specific OEM. | | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 100 | 7.3.2.5.5 | 40 | | Endpoint Security | Which method of service is acceptable to the department? Cloud based or Client-Server on premise model, please clarify | | The existing architecture for endpoint security includes TrendMicro and Symantec, which are managed by DCO (Data Centre Operations). In order to prioritize data centre security, a client-server on-premise model will be preferred. |
| 101 | 7.3.2.5.6 | 41 | | Integrated Building Management System (IBMS) –<br>PSDC is using IBMS for monitoring of all non-IT equipment (energy meter, DG set parameter, UPS parameter, FAS, WLD, VESDA etc.) using Siemens software (DIGIGOCC) and same is required to be upgraded / replaced. | | | As per RFP |
| 102 | 7.3.2.9 | 42 | | The specifications given in Annexure - B for the non-IT components are applicable only in case a new component is required to be installed or existing component is required to be replaced. | Please refer to Point 7.3.2.5.6 and 7.3.2.9. In Annexure B, whole specifications of BMS are given but there is a contradiction in 7.3.2.5.6 and 7.3.2.9. Please clarify | | Refer Corrigendum |
| 103 | 7.4.13.11 | 46 | | Service Provider shall provide a tool-based asset management system accessible through PSDC website. The Asset Management System should have the capabilities to get all desired reports without any delay | **1.** The asset management is also asked in EMS at 7.3.2.5.3. The same is to be linked to the website or it is to be created separate. Please clarify.<br>**2.** The asset management is also asked in EMS at 7.3.2.5.3. The same is to be linked to the website or it is to be created separate. Please clarify | | Solution to be provided by bidder as per RFP. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 104 | 7.4.42.1.5 | 67 | | Service Provider shall provide OEM support till End of Support of equipment is declared from the OEM. Post that service provider can provide third party support and SLAs will be applicable in both cases. | **1.** If the equipment goes down and its back to back OEM support is not available and has to be replaced with higher specification of new equipment then it is possible that new equipment may not be compatible with old neighbor equipment. What is the DCO supposed to do if in case one equipment goes down in an HA formation? Please clarify.<br>**2.** If the equipment goes down and its back to back OEM support is not available and has to be replaced with higher specification of new equipment then it is possible that new equipment may not be compatible with old neighbor equipment. What is the DCO supposed to do if in case one equipment goes down in an HA formation? Please clarify | | Refer clause - 7.4.40. |
| 105 | TQ4 | 17 | | No. of certified Data Centers managed by the bidder in last 10 years: -<br><br>4 Marks for each Uptime Tier-II or TIA-942 Rated 2 Data Centre<br>OR<br>10 Marks for each Uptime Tier-III or TIA-942<br>Rated 3 Data Centre<br>OR<br>20 Marks for each Uptime Tier-IV or TIA-942 Rated 4 Data Centre | No. of certified Data Centers managed by the bidder in last 10 years: - 1 to 2 Data centers: 10 Marks<br>3 to 4 data centers: 15 Marks<br>More than 4 data centers: 20 Marks | | As per RFP |
| 106 | 7.4.39.4 | 65 | Asset Management Services | Perform software license management, notify the DGRPG on licensing contract renewal. | Please provide the list of softwares for which you would like to do/perform software licenses management? | | To be obtained by service provider in HOTO. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 107 | 7.4.39.6 | 66 | Asset Management Services | The tool-based asset management system to be accessed by DGRPG through PSDC website should have the capabilities to get all desired reports without any delay. | Please provide the desire reports which you would like to fetch from Asset Management tool? | | As per standard industry practices. |
| 108 | Annexure - B | 153 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | The proposed EMS solution should be an integrated, modular and scalable solution from single OEM (i.e. all EMS components from single OEM) to provide comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ helpdesk \trouble ticketing system & SLA monitoring functionality and to meet all requirements mentioned in tender. | Please rephrase the statement as:<br>1. The proposed EMS solution should be an integrated, modular and scalable solution from single OEM (i.e. all EMS components from single OEM) to provide comprehensive fault management, performance management, traffic analysis, IT service desk\ helpdesk \trouble ticketing system & SLA monitoring functionality and to meet all requirements mentioned in tender. | Since Business Service Management (APM) is not the standard feature of EMS and there are APM specific OEM in the market, hence requesting Business Service Management to be removed from this compliance point. | As per RFP |
| 109 | Annexure - B | 153 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | Proposed solution should have Out-of-the-Box connectors/ probes/ Rest API's to integrate with multiple EMS solutions, including industry standard solutions from top 10 market leaders for EMS and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions, to provide an integrated topology and event views and reports to the operator. | (1) Please provide the Top 10 Market leaders solution names for EMS so that we can check whether we have Out-of-the-Box connectors/ probes to integrate with to be proposed EMS solution.<br><br>(2) Please provide the existing EMS solution names along with the version details which you would like to integrate with proposed EMS solution?<br><br>(3) Please provide the Use Cases for the integration with 3rd party EMS Solution? | This information will help the OEMs to proatctively provision necessary connectors/integrations in the EMS solution during the solution build up stage at the time of | Compatible to be ensured with major market leaders. Rest solution to be provided by the bidder. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 110 | Annexure - B | 153 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | 7. Proposed EMS/NMS solution must be ISO 27001:2013 certified to ensure security compliances. | Please rephrase the statement as:<br>To ensure the proposed software is secure, it should have ISO 27034 certification from a verification or certification agency from Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte recognized. | ISO 27034 standard helps organizations integrate security controls in their software through their software development life cycle, by defining security frameworks & vulnerability management processes. So, a software developed adhering to ISO 27034 standard when used, it protects customer assets from potential cyber breaches & security threats while complying with the Application security standards. As one of the medium to breach a Data Centre is by targeting third party COTS products and implanting trojans, so ensuring as much 3rd Party COTS products used comply to Application Security standards will ensure that those specific software is protected from external security threats, and when certified by reputed auditors like Schellman/KPMG/PwC/Ernst & Young/Deloitte, will only ensure that the audits are conducted diligently and are from a trust worthy source. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 111 | Annexure - B | 154 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | 9. Proposed solution must have at least 3 deployments in Central Government/Public Sector/State Govt./PSU`s/Large Enterprise, out of which one should be in a DC environment, monitoring & managing 10,000+ nodes/servers/endpoints across these three deployments. | Please rephrase the statement as:<br>Proposed solution must have at least 3 deployments in Central Government/ Public Sector/State Govt./PSU`s out of which one should be in a DC environment, monitoring & managing 10,000+ nodes/servers accross these three deployments. | EMS/NMS tool's responsibility is to monior and manage the IT Infrastructure that comprises of both network nodes and Servers in a Data Center. Even when we refer to the current RFP's EMS/NMS Specification, it also mentions the same i.e., monitor and manage the Network nodes and Servers, and as endpoints are never managed by EMS/NMS, so the same is not asked under the EMS/NMS section. Hence, when a product is evaluated basis its successful deployment and running, relevent monitoring and managing experience should be asked i.e., nodes and servers only and not endpoints, as endpoints do not fall under EMS/NMS category. This will ensure relevant experienced solutions are evaluated which is specific to Network Nodes and Servers as asked in this RFP and that to in similar field which in this case is Cental Govt./State Govt. as the current enduser is a State Govt. entity. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 112 | Annexure - B | 158 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | The proposed helpdesk tool must be ITIL 4 certified. | Please rephrase the statement as:<br>“The proposed Helpdesk tool must be ITIL 4 certified on Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management. The certification copy must be submitted.“ | In the corrigendum there is a mention that Helpdesk tool must be ITIL 4 certified but there is no mention of on which all practices it should be ITIL 4 certified. To brief, there are 22 Practices covered under the ITIL 4 certificate and different OEM Helpdesk tool based on what area of service they expertise on are certified on those specific practices. In a Govt. DC environment the minimum practices used for creating any workflow or process require Incident management, Problem Management, Change Enablement, Knowledge Management, IT Asset Management , Service Configuration management, Release Management, Service Desk and Service Request Management. So, asking for atleast certified on these pactices will ensure the Helpdesk tool supplied will have these workflows or process framework available out of the box for DC operator to use, otherwise you will be dependent on the OEM to develop and create these frameworks in the Helpdesk tool and if at all that tool has the | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 113 | Annexure - B | 153 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | EMS - Generic Query | Requesting customer to provide the following volumetric for Infrastructure volumetric count?<br>Please confirm the infrastructure volumetric count:<br>1. No. of network devices to be monitored (SNMP/ICMP)?<br>2. Total no. of Physical servers?<br>3. Total no of Virtual Servers?<br>4. Total nos. of DB OS instances to be monitored?<br>5. Total nos. of Middleware OS instances to be monitored?<br>6. Number of application business critical transactions to be monitored?<br>7. How many Page Views (in Million) for real user monitoring?<br>8. Total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system?<br>9. Helpdesk Analyst Type - Concurrent or Named?<br>10. Total no. of Client OS instances (desktops/laptops) for asset management & tracking?<br>11. Any specific Integrations with EMS/NMS solution?<br>12. Total node counts for Integration with EMS solution? | **Reason:** This will provide all the qualified EMS OEM's to participate equally technically and commercially. | Please refer RFP |
| 114 | Annexure - B | 153 | A) EMS/NMS Specifications for 05 Years warranty and AMC support: | EMS and Helpdesk Solution Architecture Query | Please clarify if EMS and Helpdesk solution is to be designed in DC (Standalone) or DC with HA (active - passive) or DC with HA (active - passive) and DR (Redundant)? | This clarification will help the OEMs to propose the required hardware sizing basis how the the EMS and Helpdesk solution needs to be installed in the DC & DR environment. | Solution to be provided by bidder as per RFP. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 115 | Annexure - B | 160 | E) Security Incident Management Solution (SIEM) | Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep inspection of logs. | Solution should encompass log, packet and end point data with added context and threat Intelligence. | Next Gen SIEM/ SOC should have SOAR capabilities rather than packet capture. Packet capture solution is a different technology and should be asked as full-fledged dedicated specification along with uses cases. hence we request you separate the packet capture solution from SIEM solution.<br><br>Deep Packet Inspection (DPI) can be achieved at Multiple levels starting from Network Firewall, Web Application Firewall (WAF), IDS/IPS etc. SIEM job is to collect these logs to keep a copy for compliance, analyzes and correlates every event that occurs across the organization every login, logoff, file access, database query to deliver accurate prioritization of security risks and compliance violations. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 116 | Annexure - B | 160 | E) Security Incident Management Solution (SIEM) | Solution should support minimum 30,000 EPS scalable to 40,000 at correlation, management. | Solution must be Sized for 30000 Sustained, 50000 Peak EPS without queuing or dropping any logs. SOAR Solution must support all devices as SIEM and no restriction on Admins. It must collect all flows from network without any limitation. The solution should be able to integrate with the existing components and the new proposed components in the infrastructure.The solution should support seamless migration of data from existing SIEM solution and should support executing reports on the data collected and managed by the existing SIEM solution.<br><br>The proposed solution should have a seamless Incident management and ticketing capability to generate and manage automated tickets for the alert events generated by the correlation engine. | Next Gen SIEM/ SOC should have SOAR capabilities. and asked spec is looking in complete | As per RFP |
| 117 | Annexure - B | 161 | E) Security Incident Management Solution (SIEM) | The solution should be storing both raw logs as well as normalized logs. Should store for 7 days and normalized data for 120 days for forensics. | PSDC need 7 days online log and 120 days Offline logs, is our under stading is correct. | | Yes |
| 118 | Annexure - B | 162 | E) Security Incident Management Solution (SIEM) | All necessary dedicated hardware (with min 12TB storage in raid 5/6) for Security Incident Management Solution should be provided. | All necessary hardware for Security Incident Management Solution should be provided. | Every OEM has diverent calculation for the hardware and storage based on the EPS conpression. Request you to kinf reprhase as below: | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 119 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | Need to be rephrase as<br>"The SIEM & Log Monitoring solution should be from a different OEM other than the Prevention Security solutions like F/W, Packet Capture, IPS, HIPS, AV, DLP. So that it can detect threats missed by other existing tools using the security defence in depth strategy." | As best practices in cyber security SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP and Encryption, application security. | As per RFP |
| 120 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | SIEM solution must support in- memory correlations or near real-time correlations. Correlations rules must trigger before writing logs in database | This feature will ensure protection against sophisticated attack & to take preventive action. | As per RFP |
| 121 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | SIEM solution must use data security by encrypting sensitive data with correlation capabilities on those encrypted fields | This feature will help protecting sensitive data while performing all correlation to provide 100% coverage on security analytics. | As per RFP |
| 122 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | Solution should have integration with threat intelligence feed (i.e. Virus Total, MISP etc) as well its own threat intelligence platform to have collaborative IOCs to enrich information for security analyst decision | This ensure out of the box integration capabilities to keep up-to-date IOCs for all unknows and better setup response actions or remediation steps. | As per RFP |
| 123 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | This ensures no surplus license cost to bidder/customer for SOAR while avail full loaded SOAR functionality throughout project tenure or active entitlement of the contract. If SOAR is not a primary requirement then native SOAR can be installed in future with just adding additional hardware. | Next Gen SIEM/ SOC should have SOAR capabilities. SOAR licenses should be native with SIEM and does not require any individual licenses for any SOAR capabilities (i.e. security analyst, playbooks etc). | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 124 | Annexure - B | | E) Security Incident Management Solution (SIEM) | Additional Point | Quoted Solution must have its presence in India for more than 8 years and must have at least 3 deployments for more than 30000 EPS in Government of India organization. At least 3 sign-off must be attached for more than 30K EPS from Government of India organization. | | As per RFP |
| 125 | Annexure - B | 157 | Network Traffic Flow Analysis System | It shall be able to capture, track & analyses traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc. | It shall be able to capture, track & analyses traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc. Solution should be able to handle 2 million flows per minute. | The sizing parameter is missing however for a data center like SDC the suggested sizing is recommended. | The total number of flows per minute can vary depending on the size and complexity of the network, the types of applications and protocols being used, and the traffic patterns and volume. So after understaning scope requirements, current ICT Infrastructure and architechture bidder are advised to propose solution accordingly after proper AS-Is study. The proposed solution shoud have minimum 10 Gbps throughput, which shall be scalable / meet future state requirement for contract duration at no additional cost. |
| 126 | Annexure - B | 166 | Application Performance Management | Storage of historical data is for problem diagnosis, trend analysis etc. Also the retention period for the same is at least 6 months. | Storage of historical data for minimum 6 month for trend analysis and packet data for 7 days on 10Gbps throughput. | Sizing was missing so included standard sizing for the solution. | Solution to be provided by bidder as per RFP. |
| 127 | 5.4 | 14 | Preparation of bid | The bids submitted by a consortium of companies/firms or any subcontractors will be rejected | Please allow consortium bids | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 5.1 | 10 | Eligibility / pre-qualification criteria | Qualification and Evaluation Criteria | Please allow the bidders to engage a Indian subcontractor who meets the criteria mentioned in the varied clauses of Eligibility and Evaluation criteria and further enter into integrity Pact or Teaming Agreement pre-bidding. | | As per RFP |
| 129 | Annexure - B | 164 | Next Generation Firewall (NGFW) | Firewall Solution throughput should have at least 50 Gbps. | Next Generation Firewall Solution throughput should have at least 50 Gbps with App-ID/AVC/Application Control and Logging enabled considering 64KB HTTP/appmix transactions | Some vendors might interpret Firewall throughput to be RAW Firewall throughput and considering NGFW appliance, majority of flows traversing through appliance will be Layer 7 So, Please mention clearly this to NGFW throughput and even defining HTTP frame size for throughput computation because throughput varies as the HTTP frame size varies | As per RFP |
| 130 | Annexure - B | 164 | Next Generation Firewall (NGFW) | Firewall Solution Threat Prevention throughput should have at least 30 Gbps. | Firewall Solution Threat Prevention throughput should have at least 30 Gbps considering 64KB HTTP transaction size ( Please mention all security services to be enabled while computing the same and even mention the desired security services ) | Considering NGFW platforms, throughput benchmarking should be defined with a clearly defined HTTP packet size with the mention of exact security services to be enabled while throughput is computed on the respective platform i.e. IPS/URL Filtering/Sandboxing/DNS Security/Logging , etc. otherwise throughput will degrade with varied packet size/security services and this will impact the appliance performance. Defining Packet size and security services will ensure the platform baselining during throughput calculations | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 131 | Annexure - B | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have at least 5 Lakh new sessions per second or minimum 3,80,000 new Layer 7 sessions per second. | Firewall Solution should have at least 5 Lakh new sessions per second or minimum 3,70,000 new Layer 7 sessions per second. | There is more than 80% degradation on the Layer 4 session count when same session count is computed with 100% traffic mix of HTTP/HTTPS | As per RFP |
| 132 | Annexure - B | 164 | Next Generation Firewall (NGFW) | Firewall Solution should have at least 32M concurrent sessions or at least 7.2 million Layer-7 concurrent sessions. | Firewall Solution should have at least 32M concurrent sessions or at least 5 million Layer-7 concurrent sessions. | There is more than 80% degradation on the Layer 4 session count when same session count is computed with 100% traffic mix of HTTP/HTTPS | As per RFP |
| 133 | Additional Clarification | | | | | Please define what security services licenses are required from day 1 as part of the BOQ bundled with the NGFW appliance | All the requirements mentioned in the RFP. |
| 134 | 6.11.1 | 30 | Subcontracting by Data Centre Operator | The service provider may subcontract non-IT work. Subcontracting of IT resources may be allowed after approval of DGRPG, however, resources to be subcontracted will be at the sole discretion of DGRPG. However, the service provider shall provide the list of services planned to be subcontracted, within 45 days of signing the Agreement or at least 45 days before the start of proposed subcontracted work whichever is later | The service provider may subcontract non-IT & IT work after approval of DGRPG, however, resources to be subcontracted will be at the sole discretion of DGRPG. However, the service provider shall provide the list of services planned to be subcontracted, within 45 days of signing the Agreement or at least 45 days before the start of proposed subcontracted work whichever is later | | Refer Corrigendum |
| 135 | 7.1.3.2 | 32-33 | Scope of Work - Upgradation of the PSDC | The selected bidder shall undertake design, supply, build, installation and commissioning of new IT & Non-IT infra. This includes, but may not be limited to, firewall upgradation, enhancing Building Management System, better structuring of cables, Fiber runner, reporting & logging software, online helpdesk, hosting request & invoice system. | KIndly Confirm the followings:<br>1. As per our understanding, Supply is also required where the respective infra has been declared End of Support (EoS) from the respective OEM.<br><br>2. Do bidder need to replace the EoS infra with same make/OEM & model. if not kindly share the functional & technical specification for the same. | | The infra required to be replaced or upgraded from the service provider has already been specified in the RFP. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 136 | 7 | 33 | Scope of Work | Load capacity per rack is to be increased from 4 KVA to at least 10 KVA. Refer section – 7.3.2 for details. DCO shall offer the site for Final Acceptance Testing (FAT). | Existing Rack & PDU may have limitation to increase the load capacity per rack. This might required Rack Replacement. In case of replacment for upgradation, Do bidder need to replace the EoS infra with same make/OEM & model??<br><br>If not kindly share the functional & technical specification for the same. | | As per RFP |
| 137 | 7.3.1.5 | 36 | Upgradation of the Data Centre | Bidder is also required to consider physical Infrastructure comprising Civil, Electrical & Mechanical works required in the Data Center. This shall also include site preparation to make it suitable for setting up a Tier III / Rated 3 Data Center based on GoI guidelines. | Transition from Tier II & Tier III DC may lead to existing infrastructure limitation. As such incident will not be the part of bidder scope. Kindly confirm | | As per RFP |
| 138 | 7.3.1.8.1 | 36 | Upgradation of the Data Centre | Scalability - All components of the data center must support scalability to provide continuous growth to meet the requirements and demand come from various user departments. A scalable SDC shall easily be expanded or upgraded on demand. Scalability is important because new computing components are constantly being deployed, either to replace legacy components or to support new missions. Details of scalability are covered component wise in the technical specifications. DCO shall be responsible for scalability as per DGRPG action plan | In case due to limitation of existing infra/App/Software scalablity issue, Request to consider as such should not be counted under of bidder responsiblity. | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 139 | 7.3.2.5.2 | 39 | Upgradation of the Data Centre | Application Performance Monitoring & Network Behaviour Analyzer (APM & NBS) - Currently, PSDC is using the Network Behaviour Analyzer solution of Checkpoint which is required to be upgraded/replaced with APM & NBS. | In case of replacement, kindly share the functional specification for the same along with list of Application to be monitored through APM tool | | As per RFP |
| 140 | 7.3.2.5.3 | 40 | Upgradation of the Data Centre | Enterprise Management System (EMS) - Currently, PSDC is using CA spectrum which helps for infra / network / services monitoring. Proposed solution should support following: - | In case of replacement, kindly share the functional specification for the EMS tool along and share the nos of EMS device license are being used. | | As per RFP |
| 141 | 7.3.2.5.4 | 40 | Upgradation of the Data Centre | Next Generation Firewall (NGFW) - PSDC is using Checkpoint 12200 firewall in HA mode and is required to be upgraded with following configurations:- 8 x 10/100/1000Base-T RJ45 ports, One network card expansion slot, 8 GB memory, 2 x 500 GB HDD, LOM card, Slide rails (22" to 32"), 1.7 (default)/5(max) million concurrent connections, 90,000 connections per second Proposed solution should be a multicore CPU architecture with a hardened 64-bit operating system and should be support Third party log analyzer tools / Log server/ Siem/event correlation module for NGFW & AntiAPT. | Kindly share the existing infrastrucutre detailed BOM to size the solution. | | Refer Corrigendum |
| 142 | 7.3.2.5.5 | 41 | Upgradation of the Data Centre | Endpoint Security - PSDC is using Symantec and Trend Micro antivirus with existing infra which is required to be | Kindly share the nos of license are currently deployed for Symantec & TrendMicro | | Approx. 400+ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 143 | 7.4.3 | 43 | Operation and Management of PSDC | The service provider shall maintain the Data Centre in line with minimum requirements as per the industry best practices to ensure an uptime of 99.982% on monthly basis post completion of HOTO. | In case the existing infra has been declared End of life and End of Support from the respective OEM/Vendor. Do we need to upgrade/replace with the same OEM/Vendor?? In case of upgrade/repalcement from other vendor, for that reason, kindly share the functional & technical specification for the same | | Refer clause 7.3.2 & 7.4.40 |
| 144 | 7.4.5 | 44 | Operation and Management of PSDC | DCO shall maintain all the running System Software (OS, Database, Antivirus, etc.) including adequate number of licenses looking to CPU / Core mentioned, updates, patches and OEM support Packs etc. valid for the project period to ensure that the system is properly updated. | Kindly Share the list of OEMs, model/ version, Edition (Standard/enterprise/Datacentre etc) and nos of license installed for OS, Database, Antivirus etc. | | Bidders are advised to visit PSDC with a planned schedule or service provider can get the details during HOTO. |
| 145 | 7.4.25 | 56 | Application Monitoring | 7.4.25.1 It should include monitoring of: -<br>7.4.25.1.1 Web/Application Servers.<br>7.4.25.1.2 Database Servers.<br>7.4.25.1.3 EMS Servers.<br>7.4.25.1.4 Antivirus Server.<br>7.4.25.1.5 Backup Servers.<br>7.4.25.1.6 VM Hosts Servers.<br>7.4.25.1.7 Web Application Services.<br>7.4.25.1.8 Application Security Certificate.<br>7.4.25.1.9 SSL Certificate.<br>7.4.25.1.10 Subdomain and Domains registration on DGRPG request.<br>7.4.25.1.11 All others (Old/New) application(s), Portal(s), Website(s), API(s), Service(s), Web/Mobile Application(s) hosted within PSDC. | Kindly share the list of application, portal, website, web/Mob app are to be monitored | | Bidders are advised to visit PSDC with a planned schedule or service provider can get the details during HOTO. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 146 | 7.4.41 | 66 | AMC of Non-IT infrastructure in PSDC | 7.4.41.1 The broad scope of work during this phase will include the following, but is not limited to: -<br>7.4.41.1.1 Bidder has to ensure the AMC for all Non-IT infrastructure components such as UPS, HVAC, PAC, Air - Conditioning System, BMS, Battery Bank, Fire Detection, VESDA, and Control System, Diesel Generator Units, lighting system, LT/HT electrical Panels, Power, UPS Battery, CCTV Surveillance systems, consumables and cabling etc. | In case the existing infra has been declared End of life and End of Support from the respective OEM/Vendor. Do we need to upgrade/replace with the same OEM/Vendor?? In case of upgrade/repalcement from other vendor, for that reason, kindly share the functional & technical specification for the same | | Refer Annexure - B for specifications |
| 147 | 7.4.42 | 67 | AMC of IT infrastructure in PSDC | 7.4.42.1.1 Bidder has to ensure the AMC for all the active and passive IT infrastructure components such as Server, Network, Storage & Tape Library etc.<br>7.4.42.1.2 List of all the IT Infrastructure in existing PSDC may be seen at Annexure – A. The bidder shall quote AMC cost for all IT components. While quoting, bidder shall make sure to eliminate the components already under AMC / OEM support for the duration such components are already receiving such AMC / OEM support. For the components whose AMC / OEM support will expire during the duration of the contract, Bidder shall quote the AMC cost from the date of expiry of such support till the expiry of the contract. | In case the existing infra has been declared End of life and End of Support from the respective OEM/Vendor. Do we need to upgrade/replace with the same OEM/Vendor?? In case of upgrade/repalcement from other vendor, for that reason, kindly share the functional & technical specification for the same | | Only IT components in the scope of tender to be upgraded / replaced by the service provider. Refer clause 7.3.2 & 7.4.40 |
| 148 | 7.4.42.1.5 | 67 | AMC of IT infrastructure in PSDC | Service Provider shall provide OEM support till End of Support of equipment is declared from the OEM. Post that service provider can provide third party support and SLAs will be applicable in both cases. | In case of 3rd Party support when direct support is not available from direct OEM/Vendor, in such case kindly exclude the SLAs for that infrastructure from the Bidder scope | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 149 | 9.5 | 79 | Project Implementation and Payment Schedule | If any additional hardware (IT/Non-IT) is added / procured for PSDC by DGRPG through any other vendor or is purchased by other user departments for co-location, Service Provider shall provide Operation and Maintenance services for such infrastructure at no additional cost. Service Provider shall not be responsible for provision of AMC of such infrastructure but vendor management, if any required, shall be the responsibility of the Service Provider. SLAs shall also be applicable on the service provider as specified under sub-section 10. Service Providers may deploy extra manpower to carry out the responsibilities to meet this requirement at no additional cost to the DGRPG. | Request to delete this clause. As this will have commercial impact on the overall bid | | As per RFP |
| 150 | Annexure - A | 103-116 | List of Existing IT Assets in PSDC | Annexure - A<br>List of Existing IT Assets in PSDC | In case the existing infra has been declared End of life and End of Support from the respective OEM/Vendor. Do we need to upgrade/replace with the same OEM/Vendor?? In case of upgrade/repalcement from other vendor, for that reason, kindly share the functional & technical specification for the same | | Only IT components in the scope of tender to be upgraded / replaced by the service provider. Refer clause 7.3.2 & 7.4.40. Please refer Annexure - A. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 151 | Annexure - A | 103-152 | List of Existing IT Assets in PSDC | List of Existing items | Kindly share the AMC/Warranty date.<br>In case the existing infra has been declared End of life and End of Support from the respective OEM/Vendor. Do we need to upgrade/replace with the same OEM/Vendor?? In case of upgrade/repalcement from other vendor, for that reason, kindly share the functional & technical specification for the same | | |
| 152 | 7.4.13.7 | 46 | | The PSDC portal must have a feature of generating invoices based on the ICT infrastructure consumed by end users at DCO level. The invoice shall be raised after approval through an online workflow to be defined by DGRPG. | What is the Amt calculation process for invoice generation? | | Invoice are to be generated as per the services consumed by the end user and rate list defined by DGRPG. |
| 153 | 7.4.14.2.8 | 47 | | Patch release update: Patch Release Update management (patch update procurement / downloading and installation of the same as soon as it is made available by the concerned OEM/company/ organization for all software components possible. At the same time the DCO has to submit a patch release update and installation report every fortnight to the DGRPG) | How will the patch release document be released to PSDC from DCO? | | As per RFP |
| 154 | 7.4.17.13 | 44 | | Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry account lockout policy, certificate policies, IPSEC policies etc. | The customer needs to provide specific instructions regarding the implementation of policies. They should clarify the timing of password expiry alerts and specify their preference for authentication, whether it should be single factor or multifactor. | | In accordance with the PSDC ISMS (Information Security Management System) security policy. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 155 | 7.4.13 | 45 | | PSDC Website: | The RFP mentions two terms, namely PSDC WEBSITE and PSDC ADMIN PANEL, which have distinct meanings. The PSDC WEBSITE refers to the application itself, while the PSDC ADMIN PANEL is a component of the application. Please confirm if our understanding of this distinction is accurate. | | Yes |
| 156 | Annexure - B | 158 | | Helpdesk and IT Service Managemen | Request to add V3/v4 certification for ITIL, Instead of only v4 | | As per RFP |
| 157 | Point 2 | 91 | | Availability of Project In-Charge/ Project Manager. | Service Provider needs to ensure that Project In-Charge/ Project Manager shall not take any leave (Max. leave allowed - 12 in a year) without prior approval from DGRPG. If resource deployed is not reporting to duty for 3 consecutive days without sanctioned leaves, the same will be treated as non- deployment for the purpose of liquidated damages calculation | Please Allow Max Leave Allowed - 18 in a year instead of 12 as this will help in resources deployment and management. | Refer Corrigendum |
| 158 | 7,2.4 | 34 | | Handing Over Taking Over (HOTO) | Site survey should be done for the entire network, inclusive of active (routers, switches, server, storage, security devices etc.) as well as passive (fibre/ copper cables, racks, cabinets, HVAC, BMS etc.) elements. The site survey report should enlist the details about the assets and their working status (working, not working, end of life, etc.), status of software's (like; license expired, license expiry date, license valid till date etc.). | In case, OEM doesn't replace the item/device /system after EOSL from OEM, bidder to provide it's own/third party AMC on best efforts basis and LD clause will not be imposed. During such period software/ firmware update, upgrade etc shall not be available. Pls confirm | Refer clause - 7.2.5.2, 7.4.42.1.5 & 7.4.40 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 159 | 7.3.2 | 38 | | Upgradation of the PSDC | The design of existing data center upgradation work will be based on but not limited to section 7.3.1 of tender. The service provider shall adhere and comply with all Tier III / Rated 3 standards within PSDC. | Is bidder need to upgrade all EOSL devices? In case Upgrade of IT Equipment is not required whether bidder can Provide/third party AMC on best efforts basis and LD clause will not be imposed. During such period software/ firmware update, upgrade etc shall not be available. Pls confirm | |
| 160 | Annexure -A | 102 | | Annexure - A | EOSL devices which were not in Annexure B | As per inventory mentioned in Annexure -A, there are some items which shall be End Of support from OEM during the contract period. Hence back to back OEM AMC can not be provided for entire contract period. We understand that such item shall be replaced with new item by PSDC before getting EOSL from OEM. Please confirm. | |
| 161 | Annexure -A | 106 | | Annexure - A Incorrect Serial Number | Incorrect Serial Number in Line no 52, 53, 54, 55 | Please provide correct Serial numbers | Provided as mentioned on the device. |
| 162 | Annexure -A | 102 | | Annexure - A | EOSL devices which were not in Annexure B | On software licenses point - we understand that bidder shall be responsible for all the software licenses mentioned in the RFP. In case any additional software license required due to change of architecture or device or system shall be procured separately by PSDC. Pls confirm. | Yes |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 163 | 10 | 81 | | SLA and Liquidated Damages | Penalty Capping Clause | Penalty Capping Clause: Maximum amount of liquidated damages shall not exceed 10% of overall Opex Cost for PSDC after FAT for 60 months value and Capital cost of SDC upgradation. | As per RFP |
| 164 | 10.6 | 82 | | SLA for Upgradation of PSDC | 0.5% of upgradation cost shall be deducted per week of delay or part thereof.<br>If the work is not completed within 20 weeks of proposed completion, DGRPG at its sole discretion may forfeit the PBG / terminate the contract.<br>(Maximum amount of liquidated damages shall be 10% of upgradation cost) | Please include: Delivery delay and liquidated damages shall limited to the undelivered portion and penalities will be caluclated on the undelivered Portion value only. | As per RFP |
| 165 | 10.6 & 10.7 | 82 | | SLA for Upgradation of PSDC & SLA for O&M of PSDC | 0.5% of upgradation cost shall be deducted per week of delay or part thereof.<br>If the work is not completed within 20 weeks of proposed completion, DGRPG at its sole discretion may forfeit the PBG / terminate the contract.<br>(Maximum amount of liquidated damages shall be 10% of upgradation cost) | Request you to kindly consider Partial Billing and partial Payment bases the delivery of the Equipment and Services. | As per RFP |
| 166 | 3.1.17 | 8 | | “Similar Work” means Setup / Operation & Management of ISO/IEC 27001 or ISO/IEC 20000 certified Data Centers. | Kindly change as:<br>“Similar Work” means Setup / Operation & Management of Data Centers. | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 167 | TQ2 | 17 | Technical Bid Evaluation | Successful completion of “similar work” (minimum 10 racks) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023.<br><br>5 marks for each project subject to a maximum<br>of 20 marks. | Kindly change as:<br><br>Successful completion of “similar work” in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023. | | As per RFP |
| 168 | 7.3.2.5.3 | 40 | Enterprise Management System (EMS) | Enterprise Management System (EMS) Proposed solution should support following: -<br>i. Asset Management<br>ii. Monitor the availability of Services<br>iii. Fault Management<br>iv. Performance Management (Server, Network, Security, SAN etc)<br>v. Security information management (analyze logs of servers, network devices) | Does the existing product CA spectrum has these features? Will any other OEM be acceptable with all these features? | | These features are considered as the basic requirements. However, if any Original Equipment Manufacturer (OEM) offers additional or advanced features, they will be considered and accepted. |
| 169 | 7.3.2.9 | 42 | Upgradation to Uptime Tier III / TIA-942 Rated 3 | The specifications given in Annexure - B for the non-IT components are applicable only in case a new component is required to be installed or existing component is required to be replaced. | Please refer to Point 7.3.2.5.6 and 7.3.2.9. In Annexure B, whole specifications of BMS are given but there is a contradiction in 7.3.2.5.6 and 7.3.2.9. Please clarify | | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 170 | 4.1.3 | 9 | Introduction | PSDC is Tier – II Data Centre and is ISO 20000 & ISO 27001 certified. It offers Shared Services (Computing and storage services), Co-location Services (Infrastructure provided by Client department) and Managed Services (Infrastructure purchased by DGR on behalf of Client department). Currently, more than 120+ applications and websites of different State Govt. Departments are hosted and running in PSDC. Many other departmental applications are in the pipeline. The current Data Center Operator is M/s Sify Digital Services Limited (SDSL). | Please note that in page no 9 clause no it is mentioned that PSDC is a Tier II Certified DC.<br><br>You may mention it as Tier II Complaint for information purposes. We do not know the gaps in your current facility and thus estimation of work to be carried out as per Tier III by the Contractor might hamper the overall cost and there could be gaps in the actual budgeting | | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 171 | 7.3.2.5.7 | 41 | Upgradation to Uptime Tier III / TIA-942 Rated 3 | Upgradation to Uptime Tier III / TIA-942 Rated 3 - PSDC is currently a Tier II compliant Data Centre. Service Provider shall undertake all the required upgradation activities, not included in the points above, so that PSDC is enhanced to Uptime Tier III / TIA-942 Rated 3 standards. Service Provider shall also be responsible for getting the certification for design part. Bidders shall provide separate rates for all the activities involved for Tier III / Rating 3 upgradation in the financial bid including that of certification. Payment for the same will be made post PSDC the certification. | Requesting to Certify a Data Center by Uptime vis-a-vis TIA has no relevance. You either have it certified by Uptime or by TIA. It doesnt make sense to mention either certification as the method of certification are completely different.<br>You need to understand the difference between a Guideline and Certification. Guidelines are not certifiable whereas Certification is Certifiable.<br>TIA is merely a guideline and Uptime is a Standard<br>Uptime is performance based Certification body unlike TIA which is a tick in the box<br>With Uptime you receive a Certificaiton and with TIA you will recieve a Conformance document<br>With Uptime you only have to pay once upfront and there are no renewal changes whereas with TIA you will have to pay annnual, biannual and renewal chanrges to maintain your validity.<br>Uptime is the only Certification body which will test your facility on 100% load before your Data Center will go live. No other agency or third party will test your facility post Design Certification.<br>Recommended Scope of Work to be included as a part of Certification work to be carried out by the Contractor or SI for ease of doing business. The Mandatory | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 172 | Defined Nature / Scope of Work to be carried out by the Contactor / SI | | Recommendation to include in RFP | Actual Scope of Work to be included in the scope of the Contractor / SI to define the nature of duties and deliverables | Request for Proposal (RFP) / Tender From M/S Uptime Institute (or) their Authorized Indian Representatives / Partners / Collaborators to Procure Tier – III Certification Services of Design Certification, Construction Certification Readiness Program, Construction Certification, Construction Monitoring, Commissioning Plan, Commissioning Script and Operations Certification Readiness Program, Operations Certification, across all phases of Project for Client's Name Data Center to be located at Mohali, Punjab, India Including all Civil & MEP Services & Works on EPC basis.<br>The Entire Development is to be Designed adhering to the local body / building norms / NBC 2016 along with compliance to Uptime Tier – III (with Tier – III Certification in all four stages i.e. During Design, Build, Commissioning and Operation of Data Centre) across all phases of the project along with ancillary services supporting the Main Certification for the Data Centre works and services. | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 173 | SDC Upgradation Scope of Work w.r.t. Tier III Certification | | Recommendations for achieving Tier III Certification | Please include these recommendations from Uptime Institute to achieve Tier III Certfication, kindly have them included in the RFP to ensure complaince as per Tier III norms. This will define the actual upgradation cost for e.g. Cost for Testing & Commissioning | 1. As you are aware, the Data Center facility shall observe Integrated System Testing on 100% Live Simulated Load condition based on preplanned Commissioning Script basis the Final IT load capacity to evaluate the performance of each and every system and sub-system to verify against the design and performance criteria and shall be witnessed / validated directly by Uptime. Uptime shall mandatorily witness and approve specific tests based on preplanned test scripts to evaluate the performance of each and every system at full load (simulated heat load banks) to verify against the design performance criteria<br>2. For the IT Load of more than 4 kW / Rack, it is recommended for follow continuous cooling to avoid any temperature variance during power change-over<br>3. Computer Room temperature should be maintained as per latest ASHRAE TC9.9 Class A1 Server<br>4. Change of Data Center Room Temperature should be as per latest ASHRAE TC9.9 guideline<br>The data center should be designed with capacity components rated at latest ASHRAE N=20 maximum DB temperature at the worst-case scenario | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 174 | Recommended Trainings for Staff & O&M Team | | Recommended Trainings for Staff & O&M Team | Training & Education for relevant staff | AOS Trained Staff - Minimum 3-5 nos in order to O&M as per Tier Standards<br>ATS Trained Staff - Minimum 1-3 nos (Management Team of PSDC)<br>ATD Trained - Bidder to have ATD Certified Designer from Uptime Institute on Board in order to Design as per Tier Standards | | As per RFP |
| 175 | 4) Data Center Infrastructure Management Systems (DCIMS) / Clause no. C | 214 | 4) Data Center Infrastructure Management Systems (DCIMS) / Clause no. C | C The system shall monitor SNMP/Modbus TCP devices and manage Inventory for at least 42 Racks. | The software solution shall support any vendor agnostic facility device to be integrated under monitoring using standard SNMP(v1/v2/v3), Modbus TCP/IP & BacNet over IP. DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet, Restful API etc. | All Vendor neutral, 3rd party devices either with SNMP V1, V2, V3, Mobus, BacNet or Restful API must be supported by propsed DCIM. | DCIM should be vendor agnostic and can take data from any standard protocol like Modbus,SNMP,BacNet,Restful API etc. |
| 176 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.1 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.1 | Any Modbus to Ethernet gateways needed to bridge existing Modbus points to DCIM monitoring system will be under the DCIM vendor scope. Commonly accepted protocol is Modbus / Modbus Tcp. Connectivity/wiring to the relevant proposed gateways will be under bidder scope hence Customer will share with DCIM vendor the connectivity schematic along with communication protocols for various I/O points needed for KPI reporting on common Portal. | Request you to kindly share the Final IO summary to size the number of gateway required | I/o Summay to help in sizing and optimizing the solution. | As per RFP, IO summary not required for DCIM requirement Vendor should visit the site to check the avaialble devices. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 177 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.2 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.2 | Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 7 years under the same OEM name, any change of ownership and name change for OEM will be treated as disqualification. | Proposed DCIM solution OEM should be engaged in the development of data center infrastructure management systems whose products have been in satisfactory use in similar service for a minimum of 10 years. Request you to kindly add - The OEM should have installed similar kind of DCIM solution for more than 100 racks in any 3 PSU/Banks/Government Institution who are registered in India and vendor should be able to provide supporting proof of the same. | DCIM being critical Monitoring tool for DC must have OEMs in this field with minimum 10 years to understand & address the pain points of IT/DC. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 178 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.4 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. C.4 | DCIM software OEM should have own dedicated Business Units within the company to handle the following: a. Datacenter Lifecycle services for Performing Regular Datacenter Audits and also help in Improving the throughput of implemented OEM solutions at client end including DCIM. b. Global scale Datacenter Service & Support Team for Implementation and troubleshooting DCIM d. Dedicated DCIM support BLOG for all clients who buy DCIM to provide anytime query escalation to Global DCIM product experts of the DCIM bidder. e. Cloud Based Datacenter Remote Monitoring Services to offer second layer of intensive coverage over Threshold Violations, Rules, Alerts arising within the DCIM. This system should have a dedicated manpower NOC from where the DCIM OEM will be handling this Remote Monitoring service. | Request you to kindly remove point "e". AS Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. Request you to kindly Include following The software solution shall also be subject to owner's policies for security without effect on the Server or Client operation.<br>·System must support import of certificate, use self-sign certificate or upload a certificate.<br>·The system shall not deploy protocols inherently susceptible to intrusion.<br>·The system shall strip all unnecessary files and services from the Web service to protect the owner from intrusions.<br>·Must support the ability to add security certificates via the user interface. The solution shall come as a package which includes application & a stable database. Database app must be known for good performance & importantly NOT proprietary in nature. All components of the software solution shall be installed and completed in accordance with the specification. Components shall include:<br>·Server software, database and Web browser Graphical User Interface<br>· System configuration utilities for future modifications to the system | Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. | Refer Corrigendum |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 179 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.1 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.1 | Proposed DCIM solution should be designed such that it can scale up to integrate Building side Infrastructure devices using SNMP, Modbus® TCP protocol or in cases where Building side devices cannot talk over IP, proposed DCIM solution can utilize Modbus to Modbus TCP gateways for cross Integrations. | Include "DCIM proposed is scalable to 5000 devices monitoring, supports SNMP V1, V2 , V3 , modbus TCP/IP, BacNet/IP & also restful API support." | DCIM being critical Monitoring tool should support all 3rd party integration along with varied IT protocols i.e SNMP, Mobus, BacNet, RestfulAPI etc. | As per RFP |
| 180 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.2 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.2 | DCIM platform should also be capable of pushing monitored device information to any Third-Party NMS system using SNMP INFORM/REQUEST procedures | Supports RestFul API , it is recommended to pull data from NMS thus ensuring layered security , however from Vertiv DCIM Push and pull both are supported ( a pre-requisitie for NMS is it should accept and open its interface to accept pushed data) | DCIM being critical Monitoring tool should support all 3rd party integration along with varied IT protocols i.e SNMP, Mobus, BacNet, RestfulAPI etc. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 181 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.3 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.3 | DCIM solution should be able to push DCIM monitored points to any third party BMS system using Modbus TCP out channel. | DCIM being critical Monitoring tool should support all 3rd party integration along with IT protocols i.e SNMP, Mobus, BacNet etc. Also backup and restore is one of the vital paratmerters, Request you to kindly include the same.<br>Supports RestFul API , it is recommended to pull data from BMS thus ensuring layered security , however from DCIM Push and pull both are supported ( a pre-requisitie for BMS is it should accept and open its interface to accept pushed data) , * during Design OEM to ensure that the gateway used in instrrumentation are multi client support thus multiple system can pull data when needed.<br>Software solution must support one click backup and restore option, thus enabling user to revert to last known good configuration of application, this feature will help operation team to bring system online as quickly as possible during any breakdown or revert to known configuration in case of any manual changes to be revert to last good working application config.<br>This option of Backup and restore must be available inside the web application itself, must have multiple backup and restore option.<br>If required, the proposed solution should | DCIM solution should be able to push/pull DCIM monitored points to any third party BMS system using Modbus TCP, RestFul API out channel. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 182 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.4 | 214 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.4 | Proposed DCIM system should be modular in nature that provides us flexibility to purchase and expand enhanced modules according to our future need. The DCIM should be able to run on a physical, virtualized server and offer Cloud based option for parallel high critical infra monitoring. | Request you to kindly remove "and offer Cloud based option for parallel high critical infra monitoring."DCIM is complete package , includes APP + DB all in one , DCIM can be deployed on Physical as well as virtual server. Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. Also cloud based offering is different application for such custom request cannot be sized in RFP stage ( scale of cloud , connectivity, SLA, location of cloud , Cost and such factors varies from cloud to cloud) | Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. | As per RFP. |
| 183 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.5 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.5 | DCIM vendor should have both Perpetual-Capex and Pay as You Use-SaaS, style licensing for DCIM solution. | Request you to kindly remove Pay as You Use Saas and include "DCIM sofware and license is perpetual in nature and license is provided to customer as perpetual ( no Pay as use license is applciable)." | DCIM sofware and license is perpetual in nature and license is provided to customer as perpetual ( no Pay as use license model is applciable). | As per RFP |
| 184 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.6 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.6 | On Premise -Monitoring setup for DCIM side should be created in such a way that all Infrastructure Site monitoring should happen using a single Monitoring system installed as Physical/Virtual appliance at one site. | please provide a site survey and detail IO summary of infra to be covered under DCIM | I/o Summay to help in sizing and optimizing the solution. I/o summary must be furnished during detailed engineering | As per RFP. IO summary not required for DCIM requirement Vendor should visit the site to check the avaialble devices. |
| 185 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.8 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.8 | To ensure a proper redundancy of the DCIM setup all software components should be VMWARE enabled so that customer can install the same onto VMWARE platform and utilize the capabilities of VMWARE Redundancy architecture for Disaster Recovery where needed. | Vmware must be provided by the customer. Request you to kindly confirm scope for VMware, Request you to kindly Include Software solution proposed should support user to deploy HA or DC/DR (high availability or redundancy) architecture, with 100% guaranteed uptime. | Vmware is in Clients scope. Please confirm. DCIM to support user to deploy HA or DC/DR (high availability or redundancy) architecture, with 100% guaranteed uptime. | Vmware should be provided by bidder |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 186 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.9 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.9 | Proposed system shall offer web services (WSDL, REST, SOAP) to allow integration of the DCIM system to third party Customization platforms. Vendor must submit a detailed Schema documentation for the same. | Request you to kindly remvo WSDL, SOAP. As WSDL & SOAP is separate services and not part of DCIM scope. | WSDL & SOAP is separate services and not part of DCIM scope. | As per RFP |
| 187 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.10 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.10 | DCIM server/VM system should allow integration of client email server via SMTP channel as well as it should support integration to SMS Gateway servers by utilizing the HTTP post Method. | Customer must have a SMS gateway?<br>· System must support https<br>· File type supported must be PEM | Customer must have a SMS gateway along with<br>· System must support https<br>· File type supported must be PEM | Accepted. PSDC will provide SMS gateway. |
| 188 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.11 | 215 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. D.11 | Proposed DCIM system should also have (an option which customer can add in future) of Cloud based analytics system and Remote Monitoring Services that proactively minimizes downtime and reduces break-fix resolution time through smart alarming, remote troubleshooting and visibility into client device lifecycle. It will help the OEM to: | Request you to kindly remvoe Cloud based analytics system & Remote monitoring servcies. Cloud based analytics system & Remote monitoring servcies is Not recommended in Data Centres because of threat of data breach. | Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. | As per RFP. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 189 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.1 | 216 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.1 | Proposed DCIM should be created in separate installations to maintain sanctity of data as follows:<br>a. Gateway/Convertor Devices: Required for connecting to third party BMS/ third party BMS controllers/field devices and building side device Integrator system.<br>b. Monitoring layer: Responsible for polling SNMP and Modbus TCP based Infrastructure devices inside the Datacenter like Rack Mount PDU, EMS systems etc.<br>c. Portal for Report and KPI display to integrate with Operations and Monitoring Layers of Datacenter.<br>D. Option of adding Cloud based data lake for Machine Learning and Advance Analytics for key critical Infrastructure UPS devices to monitor UPS wear and tear.<br>e. Datacenter Inventory Management to include Cage, space, Management. It should be scalable to include Capacity Planning and Thermal Imaging options. | Request you to kindly remvoe EMS Systems etc, and remove D. Option of adding Cloud based data lake for Machine Learning and Advance Analytics for key critical Infrastructure UPS devices to monitor UPS wear and tear.<br>Cloud based data lake for machine lerning...EMS is Enterprise management system is not a part of DCIM , it is a part of IT assets ( CPU,Memory, HDD,etc). Cloud DCIM is not recommended and supported. Also Cloud based system & remote monitoring services is not recommended in Data Centres because of treat of Data Breach. | Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. | As per RFP. |
| 190 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.5 | 216 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.5 | DCIM Monitoring Layer server/VM system should allow integration of client email server via SMTP channel. | Request you to kindly Include Dependent on access level, manage the event through acknowledgements, deletions, sorting rules and viewing alarm notes.<br>· Alarm console and alarm pop up window<br>· Audible system sound alert for alarm condition<br>· E-mail | Customer must have a SMS gateway along with<br>· System must support https<br>· File type supported must be PEM | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 191 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.7 | 216 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.7 | DCIM Monitoring Layer should allow for Auto Timed/Scheduled Report Emailing to selected audience on required key performance indicators. These Reports should be mailed to relevant users as CSV format. | Request you to kindly Include IT Assets: The solution includes an asset database. IT Assets are representations of a physical rack assets that will be associated to IT Racks within the software. These assets are created within a dedicated assets feature. The assets feature contains a detailed list view of assets. The asset feature shall provide the following capabilities:<br>· Asset database which is sortable, filterable and searchable by key asset data<br>· Add assets – manually or via CSV import<br>· Edit assets individually or by group<br>· Support of assets within assets (blade server enclosures, as an example)<br>· Export & import of existing asset database<br>· Ability to assign IT assets to IT racks<br>· Asset tab within the Rack View to visually display IT assets within each IT rack | | As per RFP |
| 192 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.8 | 217 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.8 | Proposed Monitoring system should have option of in-built integration to 24x7 Remote Monitoring Services from the same OEM who is providing the DCIM. This service shall be enabled SaaS based pricing option to us, so that the service can be enabled or disabled on need basis. This service should offer us APP based notifications of any critical alerts and support from OEM support team on APP Chat to troubleshoot the device issues. | Request you to kindly remove this point. Saas based pricing option etc. Built ins Remote monitoring services is not a Part of DCIM software , this is a Separate service ( customer must purchase this service separately , the contract and pricing for this service is a separate line item and not a part of intial RFP) | DCIM sofware and license is perpetual in nature and license is provided to customer as perpetual ( no Pay as use license model is applciable). | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 193 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.9 | 217 | Data Center Infrastructure Management Systems (DCIMS) / Clause no. F.9 | To ensure data security for any vendor proposing cloud Based solution following rules would apply:<br>1. Flow of information over IP will be allowed using HTTPS TLS 1.2 encrypted outbound connections on port 443.<br>2. All connections from the Cloud based monitoring gateway to OEM DCIM Monitoring cloud should be validated using an industry standard 2048-bit RSA certificate and data is encrypted in transit using 128-bit AES encryption.<br>3. To prevent unauthorized or even malicious access to OEM -DCIM Cloud system, all parts of the cloud engine should be protected by state-of-the-art firewalls. In addition, this cloud network should be configured to only allow access from specific sources (using Access Control Lists), and only a limited set of authorized personnel to have access – and only through multi-factor authentication. Preference will be given to systems offering Mobile based OTP Two factor authentication. | Request you to kindly remove point F.9. Cloud based service. Cloud based analytics system & Remote monitoring servcies is Not recommended in Data Centres because of threat of data breach. | Cloud based DC Remote monitoring is Not recommended in Data Centres because of threat of data breach. | As per RFP. |
| 194 | Data Center Infrastructure Management Systems (DCIMS) / Clause - OEM Qualifications | 217 | Data Center Infrastructure Management Systems (DCIMS) / Clause - OEM Qualifications | ISO9001, ISO 14001, ISO 50001 | 50001 OEM Specific. Request you to kindly remove 50001 and Allow ISO 9001 & 14001 , please add 27001 for ISMS security which is a must for larger participation | ISO27001 has guidelines similar to ISO 50001 but also emphasis on information security management system (ISMS) . Allow ISO 27001 / ISO 50001. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 195 | Addional Point | | Addional Point | | Tenancy : Proposed solution must support active directory or LADP integration. Proposed solution must have an inbuilt feature to support multiple internal departments by mapping them against tenant ID, thus it should provide information regarding power used, capacity used by a internal department or users | LDAP & AD integration is vital in DC enviroment to authenticate, permit, restrict, read-write features for different groups, applications etc. within same DC. | As per RFP |
| 196 | Addional Point | | Addional Point | | Configuration of operators: User names and passwords: · Permissions: The Permissions field allows administrators to set access level for different users. Permissions include the following options:<br>o Read/Write: Full read access and full write access to the entire system.<br>o Read Only: Full read access but no writes or changes may be done.<br>o Read/Acknowledge: Full read but no write or changes may be done, except to alarm database for acknowledging alarms. System owner shall have the ability to assign combinations of roles and privileges to users that define access levels.<br>o User password expiration<br>o Auto-log off period<br>o Audible Alerts | AAA (Authentication , Authorization & Accounting) are vital parameters within DC to identity of users or devices attempting to access the DCIM system, authorization determines the level of access and privileges they have within the DCIM system & logging and tracking of user activities within the DCIM system. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 197 | Addional Point | | Addional Point | | Events and Alarms: Events and alarms associated with a specific system, area or equipment shall be displayed on the main site view and/or within an embedded alarm console. The solution must have native capability to alarm on all connected devices. The alarm system shall have multiple alarm types depending on the severity level. Users must be able to drill down through views to locate alarm sources. The alarm should be accessible from the device level. Events, alarms and reporting actions shall have the following capabilities: Alarm Console: Capable of displaying the following information for each alarm that has occurred in the system: Alarm State (with associated status color), Site, Device, Circuit, Tenant, Point, Point Type, Point Unit, Source, Last Alarm, Acknowledge Requested, Acknowledge State, Last Acknowledgment, Last Acknowledged By, Last Return to Normal, Last Update, Alarm Class, Warning Class, Message and Notes. The Alarm Console must also provide a link to the Site, Device and Point. User Definitions: Users must be able to choose the thresholds (high and low) for when an alarm and/or warning will activate, along with the points for the | SNMP Traps, notifications and other critical Alarms are very useful in DC envirorment for real time Enviromenta Monitoring, breaching of pre defined threshold, idetifiying nuisance alarms and collectively building up predective action to avoid major failure and prevent downtime. | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 198 | 14) Technical specifications for IPDUs | 310 | 14) Technical specifications for IPDUs | - Intelligent Rack PDU should be 3 phase 16AMP must support 11KW load have minimum 18 no's C13 and 6 no's C19 socket for power distribution to IT equipment and should be mounted vertically in rear of rack occupying 0U space, UL certified. | Detailed technical specification points are missing, request you to kindly consider the below latest tehcincal specifications for IPDUs.<br>Each rack should have 2 IPDU to be connected to the two different UPS sources A and B individually, both IPDUs in each rack should have different chassis color for identification of UPS source. iPDU should be 16A, 400V, 3-phase to support the 11 kW load per rack. IPDU should have minimum 24 numbers of UL Certified outlets of hybrid nature which can be utilized as either C13 or C19 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords. Input cable must be minimum 3-meterlong, and input industrial plug should be IEC60309 and must be Splash proof IP44.<br>The IPDU should be high temperature grade, operating temperature up to 60°C.<br>All IPDU should have magnetic circuit breakers for overcurrent protection & it should be as per the IEC guidelines.<br>The IPDU should have color coded outlets based on circuit breakers color for easy identification of circuits for quick troubleshooting and ease in maintenance.<br>Monitoring parameters – The IPDU should have monitoring capability at the | Allow CE/UL certifications for larger OEM participation. Also please consider detailed iPDU specifications for strip level monitoring for remote access of vital paramerts i.e V, A, W, kWH, PF & seamless integration with proposed DCIM. Single sensor to monitor real time Temp. humidity, dew point, Air flow inside the Rack is must. All iPDUs & Sensors to be mapped with DCIM to highlight hot pockets or over colling within DC space. Also suggest for combi/hybrid sockets for ease of C14 & C20 power cords invententory management. High retention sockets to avoid accidental dislodging of power cords. Color coded outlets based on Circut breakers for easy identification of circuts for quick maintenance & troudbleshooting. IPDU should have the provision to auto discover all the similar IPDU's in the network by logging in a single IPDU to push the upgrades and configuration files to all the desired IPDU's in the network without any additional software. | Refer Corrigendum |
| 199 | Addional Point | | Addional Point | | Rack technical specifications is missing in the RFP, Request you to kindly share the rack specification | | As per RFP |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 200 | 3) UPS Critical Load / Cluase no. i | 203 | 3) UPS Critical Load / Cluase no. i | The UPS should be provided with phase sequence correction at input | Request you to kindly change this clause as "The UPS should be provided with phase sequence protector instead of corrector. | In a critcal facility no equipment including UPS system experience the phase reversal ,as there is a phase sequence check at Facility entrance. | Phase sequence correction is a critical aspect for any Data center application hence this is highly recommended so internal or external phase sequence corrector required. |
| 201 | 3) UPS Critical Load / Cluase no. K. / Modes of Operation: e | 204 | 3) UPS Critical Load / Cluase no. K. / Modes of Operation: e | Maintenance bypass -In maintainence bypasss the load is supplied with unconditioned power from the manual maintenance bypass input switch provided in a separate enclosure with each UPS | Request you to kindly add "Maintenance bypass should be default feature of UPS." | Maintenace Bypass should be Inbuilt feature of UPS. | As per RFP |
| 202 | 3) UPS Critical Load / Cluase no. n | 204 | 3) UPS Critical Load / Cluase no. n | The UPS shall be provided with oscilloscope for measuring and recording input/output voltage & current waveforms in the event of any abnormal or alarming situation arises. In-case it is not available within the UPS, then two numbers of 3 Phase Power Meters (one at Input & one at Output) shall be provided along with the UPS system which can capture the Waveforms Triggered during the failure event. | This is vendor specific specification. | UPS Indiactes power reading and not the energy reading. And this feature dosent help in the performance of the UPS. Basic Monitoring of the UPS is displayed on UPS LCD. | As per RFP |
| 203 | 3) UPS Critical Load / Cluase no. p | 205 | 3) UPS Critical Load / Cluase no. p | UPS shall have built-in feature to test UPS at 100% Load without the need of any external Load Bank. Incase this feature is not available within the UPS, Vendor shall provide an External Load Bank equal to UPS Capacity which will be kept at the site till the end of Warranty period. | Request you to kindly consider "Load bank shall be provided for FAT/SAT Either an inbuilt/external Load bank should be available." | "Keeping an load bank on site till the end of the warranty" How does it help in your operational performace and what do we want to achieve out of this arrangement. | Refer Corrigendum |
| 204 | Precision Air conditioner (PAC) / Cabinet Construction | 198 | Precision Air conditioner (PAC) / Cabinet Construction | Outside panels shall be coated with grey epoxy-polyester paint, which guarantees the long-term durability of their original features. | Shall Be as per OEM Design. This is OEM Specific | | As per OEM standard only OEM need to guarantee the long-term durability if their original features. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 205 | Precision Air conditioner (PAC) / Fans | 198 | Precision Air conditioner (PAC) / Fans | The directly-coupled EC electric motor is of the three-phase (or single-phase in outside-rotor type protection grade IP44), offering the opportunity for speed adjustment by means of controller and complete with thermal protection (klaxon) inside the electric motor winding. Using this type of fan with a highly-reactive fan wheel instead of the one with forward curved blades enables you to reach higher useful static pressures (up to 350 Pa) | OEM Specific , EC Fan should be used | | As per RFP |
| 206 | 2) Precision Air conditioner (PAC) / Compressor | 199 | 2) Precision Air conditioner (PAC) / Compressor | PAC should be equipped with Latest-generation hermetic / variable scroll compressors (air-cooled DX versions), characterized by a high COP (coefficient of performance) and consequently also a high energy efficiency. | Kindly Clarify if Variable Scroll Compressor ( Inverter/ Digital) is required which is latest energy efficient Also Fixed Scroll will not be acceptable. Kindly clarify | | As per RFP, PAC should be equipped with latest-generation hermetic scroll / variable scroll compressors |
| 207 | 2) Precision Air conditioner (PAC) / Compressor | 199 | 2) Precision Air conditioner (PAC) / Compressor | There should be a minimum 2 compressors and minimum 2 circuits per PAC | Request you to kindly consider as "Should be as per OEM Design" . With latest Variable Scroll technology Dual Compressor not required , Additional Capital Expenditure. | | As per RFP |
| 208 | | 199 | | Liquid receivers with safety plugs shall be installed inside the unit (in the air-cooled DX versions). | Required only if piping length is more than 60 RMT from IDU to ODU , Should be optional if Required. | | Yes |
| 209 | 2) Precision Air conditioner (PAC) / Refrigerating circuits (air cooled DX versions) | 199 | 2) Precision Air conditioner (PAC) / Refrigerating circuits (air cooled DX versions) | Circuit should also include Liquid Line Solenoid Valve (LLSV) & Non-Return Valve (NRV) in the discharge line for inherent capability to take care of long length piping between indoor & outdoor units and for safe operation of compressors. | Can Be installed in low Side externally, if piping length is Long , Not necessirily required inside the unit . | | LLSV and NRV is required pls provide internally or externally |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 210 | 2) Precision Air conditioner (PAC) / Humidifier | 200 | 2) Precision Air conditioner (PAC) / Humidifier | Immersed-electrode humidifier (minimum 8kg/hr rating) for modulating sterile steam production with the automatic regulation of the | Latest Genration infrared humdifier Should be allowed, Which is independent of water Quality and consumes nominal power , and is not consumable . Rating should be as per oem Design . | | Open type Infrared Humidifier may cause water spillage in the data center in case of sensor failure that's why bottle type electrode humidifier required please treat this clause as unchanged. |