

Response to Queries (RTQ) – Tender Reference No.: DGRPG/PSDC_DCO/2023/3							
SN	Tender / ATC Clause No.	Page No.	Tender / ATC Clause	Tender / ATC clause details/specification	Amendment Sought / Suggestion	Justification	PSeGS response
1	7.3.2.5.3	40	Enterprise Management System (EMS)	Currently, PSDC is using CA spectrum which helps for infra / network / services monitoring. Proposed solution should support following: - i. Asset Management ii. Monitor the availability of Services iii. Fault Management iv. Performance Management (Server, Network, Security, SAN etc) v. Security information management (analyze logs of servers, network devices)	We request to remove SIEM from EMS and ammend the clause as below: The Proposed solution should support following: - i. Asset Management ii. Monitor the availability of Services iii. Fault Management iv. Performance Management (Server, Network, SAN etc)"	As per below Clause mentioned in Annexure - B Technical Specifications - IT Components; 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. We understand that Security information & event management,UBA,APM etc. are not part of EMS and are sparate 3rd party solution, hence we request to remove this requirement from EMS and amend the clause accordingly.	As per RFP

2	Annexure B.A.7	152	EMS/NMS Specifications for 05 Years warranty and AMC support	Proposed EMS/NMS solution must be ISO 27001:2013/ ISO 27034 certified to ensure security compliances.	We request to amend the clause as : "Proposed OEM of EMS/NMS solution must be ISO 27001:2013/ ISO 27034 certified to ensure security compliances. "	We request to amend this clause as per standards for wider participation.	As per RFP
3	Annexure B.B.3	153	Server & Application Fault, Performance Monitoring Management	There should be a single agent on the managed node that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations.	This is OEM specific we request to relax this clause below for wider participation. "The solution should be agentless/agent based on the managed node, that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide actions like notifications, email alerts etc."	This is OEM specific, hence we request to amend this clause for wider participation.	As per RFP
4	Annexure B.D.I.4	157	Helpdesk and IT Service Management	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.	We request to amend this clause as below for wider participation. "The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, SLA, Problem, Change, Knowledge Management, Asset Management and CMDB."	Release management, is a process within software development and , hence we request to relax this and amend the clause with required relevant processes.	As per RFP

5	Annexure B.D.I.3	157	Helpdesk and IT Service Management	The proposed helpdesk tool must be ITIL 4 certified.	We request to remove this clause of foreign OEM certification.	ITIL V4 certificate is a foreign certificate which is under restrictive criteria as per GOI - MII Policy. As a part of "Make in India" initiative, MoUD has advised that restrictive clauses that work against the Indian companies should be modified or removed. Such conditions include - requirement of foreign certifications such as ITIL/Pink Verify etc. (Refer GoI policy - referring office memorandum, Ref no.: P-45014/33/2021-BE-II (E-64737), dated: 20th December, 2022 from Govt. of India.	As per RFP
6	7.4.31.5	61	Help Desk Services & Monitoring Team	The helpdesk solution should have an inbuilt workflow for helpdesk automation from Data Centre Entry from Reception to Issuance a visitor/Official Pass for PSDC premises.	We understand that this is part of physical standard operating procedure along with visitor/official management passes that shall be managed physically and is not a part of the ITSM, Kindly confirm.	We understand that this is part of physical standard operating procedure along with visitor/official management passes that shall be managed physically and is not a part of the ITSM, Kindly confirm.	As per RFP
7	Annexure B.B.12	154	Server & Application Fault, Performance Monitoring Management	Alarm Filtering should allow flexible filtering rules for PSDC staff to filter the alarms by category, severity, elements, duration, by user, by views, by geography or by department.	This is OEM specific we request to relax this clause below for wider participation. "Alarm Filtering should allow flexible filtering rules for PSDC staff to filter the alarms by category, severity, elements, by location/geography".	This is very specific, hence we request to amend this clause to make it generic for wider participation.	As per RFP

8	Annexure - B.D.II.2	157	Helpdesk and IT Service Management	Must allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.	Release management, is a process within software development. Hence, we request to amend this clause as below for wider participation. "Must allow creating and applying various operational level parameters to Incidents,Requests, Changes, Problem,Knowledge , SLA Mgmt."	Release management, is a process within software development, hence we request to amend this clause with relevant processes for wider participation.	As per RFP
9	7.3.2.5.2	40	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. Proposed solution should support a user-defined dashboard for instant visualization of an application's condition, customize-able via widgets. User customization and embedding of widgets is up to the user, including the application performance index, 5 slowest transactions, and other summary information and statistics relative to a definable time interval (past x hours/days).	We understand that APM, NBS and SIEM are 3rd party solutions and are not a part of proposed EMS, Kindly confirm.	APM, NBS and SIEM are not standard EMS components and should be part of 3rd party solutions.	Yes

10	Annexure B.B.7	- 153	Server & Application Fault, Performance Monitoring Management	The system should have context-based analysis and forecasting based on performance data with automated policy deployment with detailed, intelligent monitoring of performance and availability data collection.	This clause is very specific, hence we request to amend this clause as below to make it more generic and allow for wider participation. "The system should have predictive analysis and forecasting for performance and traffic analysis along with intelligent monitoring of performance and availability."	This clause is very specific, hence we request to amend this clause for wider participation and make it more generic.	As per RFP
11	Annexure B.A.9	- 153	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+ network nodes/servers 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 in single deployment.	To ensure a proven and trusted solution is considered, we request to consider the amended reference for deployment.	As per RFP
12	Additional Point	-	-	-	OEM of the proposed EMS/NMS should have CMMI Level 3 certification. OEM shall facilitate the validation of CMMI L3 Certificate from CMMI Institute.	Considering the criticality of the project and to ensure trusted & quality driven solution, the OEM of EMS/NMS should have cmml level 3 certificate.	As per RFP
13	Additional Point	-	-	-	The proposed EMS software should have qualified Security verification certificate by STQC (Ministry of Electronics & Information Technology) or any other Government agency from the list of CERT-IN empanelled Information Security Auditing organization for testing and issuing the certificate /clearance.	Since security is of paramount importance, we request that the proposed EMS solution should have security certification.	As per RFP

14	Annexure B.G.1	- 163	Next Generation Firewall (NGFW)	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.	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.	Ports requirement with immediate devices should be met by 16 x 10G ports on the other hand, 40G ports requirement is on higher side. Therefore, request you to reconsider the changes as suggested.	As per RFP
15	Annexure B.G.5	- 163	Next Generation Firewall (NGFW)	Solution must have at least 25 Gbps IPsec VPN throughput.	Solution must have at least 45 Gbps IPsec VPN throughput.	As per clause no 36, minimum 1000 site to site VPN tunnels and minimum 5000 client to site are require but throughput ask for VPN i.e. 25 Gbps is not in line with the requirement. Average user require minimum 5 Mbps of speed to access data center remotely which in turn require minimum 5 Mbps x 5000 Users = 25 Gbps and additionally site to site bandwidth require should be minimum 20 Mbps x 1000 IPsec VPN = 25Gbps which in addition require minimum 45 Gbps of IPsec throughput. <a href="https://dataprot.net/guides/vpn-internet-speed-recommendation">https://dataprot.net/guides/vpn-internet-speed-recommendation</a> .  Therefore, request you to reconsider the IPsec VPN throughput as suggested.	As per RFP

16	Annexure B.G.9	- 163	Next Generation Firewall (NGFW)	Firewall solution based on upto 3U space design form factor.	To be deleted.	Restricting scalable solution for Data Center future requirement or restricting Data Center scalability.	As per RFP
17	Annexure B.G.15	- 163	Next Generation Firewall (NGFW)	Proposed Solution must at least 10 Virtual systems such as logical, separately managed firewall instances within a single physical firewall, with each virtual system's traffic kept separate and scalable virtual systems.	Proposed Solution must at least 10 Virtual systems such as logical, separately managed firewall instances within a single physical firewall, with each virtual system's traffic kept separate and scalable upto 150 virtual systems.	Virtual system segregate network traffic either coming from internet or from internal data center. Considering the State Data Center, the traffic will reach to data center from all over the State and therefore, virtual system should be scalable and supported by the firewall without affecting the existing policies and network traffic of data center. Request to reconsider the changes as suggested.	As per RFP
18	Annexure B.G.20	- 164	Next Generation Firewall (NGFW)	Proposed solution will able to provide accurate identification and classification of all devices on a network, including never-before-seen devices.	To be deleted.	OEM Proprietary Specification. 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. Request to reconsider the changes as suggested for wider participation.	As per RFP

19	Annexure B.G.21	- 164	Next Generation Firewall (NGFW)	Proposed Solution must have lot Device security feature which support ML-based anomaly detection.	To be deleted.	OEM Proprietary Specification. 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. Request to reconsider the changes as suggested for wider participation.	As per RFP
20	Annexure B.G.30	- 164	Next Generation Firewall (NGFW)	Should have more than 10,000 (excluding custom signatures) IPS signatures or more.	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.	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. Therefore, request you to reconsider the changes as suggested.	As per RFP



21	Annexure B.G.33	- 165	Next Generation Firewall (NGFW)	The firewall should be supported Third party log analyzer tools and Log server and SIEM /event correlation module for NGFW & Anti APT.	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.	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
22	Annexure B.G.42	- 165	Next Generation Firewall (NGFW)	The management platform must provide centralized logging and reporting functionality. The management platform must provide a customizable dashboard.	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.	MITRE framework provides holistic 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

23	2	5	Document Control Sheet	-	Request for Sharing the total estimated value of the tender/work.	Railtel being PSU (Govt. Organization) needs to get the primary estimates vetted from its respective finance department. Absence of estimated value of work in this RFP is restricting Railtel Marketing department. to get the approvals from finance.	As per RFP
24	5.10.1.TQ2	17	Technical bids evaluation	<p>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.</p> <p>5 marks for each project subject to a maximum of 20 marks.</p>	<p>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.</p> <p>5 marks for each project subject to a maximum of 20 marks.</p> <p>OR</p> <p>Successful completion of “similar work” (minimum 20 racks) in government (departments/ boards/ corporations/ PSUs/ Societies) or Large reputed Enterprise in the last 10 years as on 31.03.2023.</p> <p>10 marks for each project subject to a maximum of 20 marks.</p>	<p>Data Centers with 20 Racks are more common in nature and certified .However Data Center with 10 Racks are catering to few or Single department and less likely in nature to be certified.</p>	As per RFP

25	7.4.44.2	68	Electricity and Diesel Management	DCO shall maintain a register for monitoring and reimbursing the diesel consumption for the DG set. Format of the register shall be to the satisfaction of the Client.	-	-	It is clarified that DCO will manage and monitor PSDC diesel and electricity requirements. Since DGRPG will directly bear the expenditure to be incurred on electricity and diesel, therefore, there will be no reimbursement.
----	----------	----	-----------------------------------	--	---	---	--