Sl. No.	Section	Clause No.	Description in RFP	Clarification sought	Additional Remark (if any)	ICSI Reply
1	PART 'A'	1	vendors having expertise to provide Complete Data Centre Operational Services (for Servers, Switches, Network devices, Routers, Firewalls and Software etc.),	We assume that the OEM support is in place and is not part of this RFP. Please confirm.		ICSI procures OEM support wherever required, and the same is decided solely by ICSI officials.
2	PART 'A'	26	experience on System Administration, Server Administration, Firewall Administration, Database Administration in SQL Servers/Oracle Database and Network Administration (Routers/Switches), on the platforms in use in the Institute	This clause requires resources with multiple skills. Please clarify if vendor can propose separate resources for Database administration and network administration. Accordingly, we suggest revision of commercial format.		Same as per RFP/Tender.
3	II	Scope of Work	The service provider will depute Two (2) Chief FMS Engineers (Level 3) at ICSI, NOIDA Office and they will be responsible of all System Administrator activities at Primary Data Center (Servers, Software's, Network, Hardware, Applications, Databases, AI tools/Apps, IT Policies, Security Policies, System Configuration, DC & DR Monitoring, Antivirus, MS O365 Email on cloud, ICSI Applications & Database deployment /Hosting/ Configuration on Cloud services (like MS Azure, AWS, etc.), Fire Walls, Websites etc.	Which applications are being used by ICSI? Is application support is in scope of bidder?		The FMS vendor shall provide proper requisite FMS platform support in coordination with Cloud service provider. Application support shall be provided by the Application Support /Developer service provider.

4	C	Maintenance Service	Service Provider will manage the onsite Helpdesk system as per ICSI working hours	The commercial format does not have provision to quote for Helpdesk. Please confirm if two resources will also act as helpdesk?		The role of the vendor is only to manage the existing systems and depute FMS engineers for providing the IT support, as ICSI already has a licensed Helpdesk system and no additional license are required from the vendor.
5	F	Service Calls	Service Provider will provide ONSITE helpdesk support to ICSI to cater to the requirements as per the scope of this agreement.	Please confirm if bidder need to quote for helpdesk resources?		Resources will be as per the RFP and there is no separate helpdesk resources are required. FMS will use exisitng Helpdesk system as Chief FMS engineer for ticketing.
6	J	Working Schedule	Data Center/Network monitoring: 24x7 online/offline	In commercial format, where to add quote for 24x7 monitoring		Same as per RFP/Tender. The quote will include 24×7 offline and online monitoring.
7	K	Upgradation of systems	Oracle Apps	The skillset require for upgrade of Oracle Apps is very different from Network / Hardware. Please confirm if we need to propose separate resources for Oracle Apps		ICSI has separate Oracle Apps team. Vender has to configure/install the Operating system platform in the servers as per the requirement of the Oracle Teams.
8	N & 8.8	Cyber Attack Prevention and Security Management	The Service Provider shall take all necessary proactive measures to protect ICSI's IT infrastructure from cyber threats, including but not limited to, ransomware, malware, phishing, and unauthorized access.	This is a separate service and can be provided through SOC service. Please confirm and update commercial format to include quote for SOC (Security Operations Center)		The scope includes proactive security measures and standard security management activities required for protection of ICSI's IT infrastructure through available Security tools/ UTM/Firewall/End Point Security software with ICSI. Separate dedicated SOC (Security Operations Center) services are not envisaged under the present scope of work. Therefore, bidders

						are not required to submit a separate commercial quote for SOC services.
9	Annexure B2	5	Bidder should have at least Four (4) years of experience in similar kind of projects (Facility Management Services for IT). Submit the documents as proof (at least one PO/WO which is within 4 years before bid submission date).	Company provide FMS support to many of our clients but in Time and Material Basis. Can you accept PO of T&M Contract? Please confirm.		As per Tender.
10	Annexure B2	11	The bidder should have at least Three (3) clients FMS contract, out of which minimum One (1) should be Central Government/State Government/ Public Sector organizations /Autonomous Bodies/ Statutory Bodies, Business house. (Please attach work order/agreement copy).	Company provide FMS support to many of our clients but in Time and Material Basis. Can you accept PO of T&M Contract? Please confirm.		As per Tender.
11	Cybersecurity	II.n	The Service Provider shall take all necessary proactive measures to protect ICSI's IT infrastructure...	Could ICSI provide the comprehensive inventory, architecture diagram, and asset count of the IT infrastructure to be protected (e.g., number of endpoints, servers, network devices, and cloud workloads)?	Required to properly size the operational effort, tool licensing requirements, and engineering deployment parameters.	Kindly refer to the scope of work and technical specifications provided in the tender document. Approx. Servers : 55, Endpoints: 500, Netwrok Devices: 150, Cloud environments: 2 instances (Applications).

12	Cybersecurity	II.n	...including but not limited to, ransomware, malware, phishing, and unauthorized access.	Are the endpoint protection (EDR/XDR) and email security gateways already provisioned by ICSI, or is the Service Provider expected to procure and bundle these specialized software tools in the commercial bid?	Clarifies licensing ownership and prevents massive unbudgeted software procurement costs during execution.	End Point protection (EDR/XDR), Email Services are on MS O365 with ATP support is already with ICSI. The existing ManageEngine OpManager shall serve as the primary monitoring tool for Data Centre Services, and the Vendor shall utilize it to the maximum extent possible.
13	Cybersecurity	II.n	...multi-layered security strategy involving regular vulnerability assessments...	What is the expected frequency of the "regular vulnerability assessments" (e.g., monthly, quarterly)? Will ICSI provide the enterprise scanning tools (e.g., Nessus, Qualys), or must the bidder supply them?	Defines operational cadence and identifies tool procurement responsibilities.	ICSI has IT Security Audit service provider and VA/PT will be done by this auditor. FMS resource has to extend their support to audit team for implimentation of suggesions and do configurations.
14	Cybersecurity	II.n	...regular vulnerability assessments...	Does the scope of vulnerability assessments include external Penetration Testing (PT), Web Application Security Testing (WAST), and API testing, or is it limited to internal automated vulnerability scanning?	Differentiates basic automated infrastructure scanning from highly technical, manual ethical hacking services.	ICSI has IT Security Audit service provider and VA/PT will be done by this auditor. FMS resource has to extend their support to audit team for implimentation of suggesions and do configurations. FMS service provider has to ensure regular pathcing, updates in the system.

15	Cybersecurity	II.n	...timely application of security patches...	Please define the acceptable SLA window for "timely application" based on vulnerability severity (e.g., Critical within 72 hours, High within 14 days). Will ICSI guarantee predefined downtime windows for patching production servers?	Protects the bidder from penalties if security patches cause application instability or if ICSI business teams refuse necessary downtime.	The SLA for timely application of security patches shall be finalized mutually with the selected bidder based on the criticality and severity of vulnerabilities, keeping in view operational requirements and business continuity. Necessary downtime windows for patch deployment on production servers shall be coordinated and approved by the concerned ICSI teams in advance.
16	Cybersecurity	II.n	...timely application of security patches…	Does patch management extend to OEM firmware updates for network/storage hardware and third-party custom business software, or is it limited strictly to Operating System (OS) patches?	Delineates system administration scope from application development/maintenance scopes.	The Vendor shall apply all security patches for software installed on hardware and all standard/general-purpose software. This requirement shall be extend to custom-developed software with advice and peior approvals from ICSI Technical Team.

17	Cybersecurity	II.n	...and the continuous monitoring of network traffic for anomalies.	Does ICSI currently operate an active SIEM/SOAR platform, or is the bidder expected to deploy a new SIEM tool? Is a 24/7/365 Security Operations Center (SOC) team mandatory for this requirement?	Continuous traffic monitoring for anomalies typically demands a fully managed SIEM tool and 24/7 round-the-clock SOC personnel.	The scope includes proactive security measures and standard security management activities required for protection of ICSI's IT infrastructure through available Security tools/ UTM/Firewall/End Point Security software with ICSI. Separate dedicated SOC (Security Operations Center) services are not envisaged under the present scope of work. Therefore, bidders are not required to submit a separate commercial quote for SOC services. ICSI is not currently operating an active SIEM/SOAR platform and does not expect the Vendor to provide any licenses for the same. In case ICSI decides to implement SIEM/SOAR in the future, ICSI will procure all licenses at its own cost, while the Vendor shall carry out the implementation.
18	Cybersecurity	II.n	The Service Provider is responsible for ensuring that all security appliances (Firewalls, IDS/IPS, Antivirus) are updated...	Could ICSI provide the exact make, model, operating version, and current support status of all existing Firewalls, IDS/IPS, and Antivirus management consoles?	Ensures the legacy hardware is capable of running updated definitions without encountering CPU/memory	ICSI have latest technology IT Security Devices like Firewall/End Point Solution all these are back-to-back support with OEM. FMS service provider has to coordinate with partners/OEM's to intact security services live and uptodate in all aspects.

					performance degradation.	
19	Cybersecurity	II.n	...updated with the latest definitions and signatures.	Who will bear the commercial costs for renewal of OEM subscriptions, licenses, and support agreements for these security appliances throughout the contract period?	Prevents major financial misalignment regarding recurring security software subscription fees.	ICSI have latest technology IT Security Devices like Firewall/End Point Solution all these are back-to-back support with OEM. FMS service provider has to coordinate with partners/OEM's to intact security services live and uptodate in all aspects.
20	Cybersecurity	II.n	...establish an Incident Response Plan to mitigate the impact of any potential breach...	Is the Service Provider expected to draft a completely new Incident Response Plan, or align operations with an existing, approved corporate Incident Response policy within ICSI?	Clarifies the scope of corporate governance documentation deliverables.	Kindly refer to the scope of work and technical requirements specified in the tender document. The Service Provider shall establish and maintain an Incident Response Plan in alignment with ICSI's requirements and applicable policies, ensuring effective incident handling and mitigation throughout the contract period as suggested by IT Security Auditors time to time.

21	Cybersecurity	II.n	...and ensure the integrity of the Data Center.	Does the scope of "Data Center integrity" encompass managing and testing immutable, air-gapped, or offline backups for ransomware recovery? Please provide details on the current backup solution.	Ensures clear demarcation of responsibilities between the IT backup team and the cybersecurity management team.	ICSI has its backup & restoration system and its polocies. ICSI will provide the Backup Strategy to the awarded bidder. The Vendor must implement the same. Any modifications to the strategy shall be decided by ICSI officials.
22	Cybersecurity	II.n	In the event of a suspected or actual cyber-attack, the FMS Engineers shall provide immediate remedial action...	Please provide explicit definition and SLA parameters for "immediate remedial action" (e.g., Triage within 15 minutes, Containment within 1 hour) for critical incidents.	Vague terms like "immediate" must be converted into quantifiable, contractually binding SLA metrics to measure engineering performance.	As per RFP/Tender.
23	Cybersecurity	II.n	...the FMS Engineers shall provide immediate remedial action...	Does "remedial action" authorize FMS engineers to isolate production environments, block network traffic, or shut down critical business services autonomously during an active threat without explicit written approval?	Establishes emergency authorization guardrails to avoid legal liabilities for operational downtime caused by containment actions.	The Vendor will suggest remedies, while the final decision will be taken by ICSI officials.

24	Cybersecurity	II.n	...document the root cause...	Does root cause documentation imply basic log collection by regular FMS engineers, or does it require certified Digital Forensics and Incident Response (DFIR) malware analysis expertise?	Deep forensic investigation requires specialized, high-tier experts whose costs exceed standard Facility Management Service (FMS) staff.	The Vendor has to perform primary root cause analysis. Whether deep forensic investigation is required or not will be decided by ICSI officials.
25	Cybersecurity	II.n	...and implement enhanced security controls to prevent recurrence.	If preventing recurrence necessitates the procurement of new or upgraded security hardware/software infrastructure, who will bear the capital expenditure (CapEx) for such controls?	Differentiates operational security hardening from capital asset additions.	The Vendor has to bear the license cost of OpManager only. Ayn Hardware/ Software licenses will be procured by ICSI.
26	Cybersecurity	II.n	In the event of a suspected or actual cyber-attack...	In case of a sophisticated Zero-Day exploit or an Advanced Persistent Threat (APT) attack where the Service Provider followed all updated protocols, will the bidder be held financially liable for business losses or data breach penalties?	Limits bidder liability for highly sophisticated state-sponsored attacks that bypass industry-standard updated signatures.	In the event of a cyber-attack, the Service Provider shall follow all updated protocols and best practices. However, in case of highly sophisticated Zero-Day exploits or APT attacks that bypass all existing security controls despite due diligence, the Service Provider shall not be held financially liable for business losses or data breach penalties. The Vendor shall provide full cooperation and implement all

						remedial measures as directed by ICSI.
27	Cybersecurity	II.n	...administrative access is strictly governed by the Principle of Least Privilege (PoLP)...	Does ICSI currently own a Privileged Access Management (PAM) or Privileged Identity Management (PIM) tool to govern administrative access, or will this be managed via native Active Directory features?	Determines if enterprise-grade tooling is available to fulfill and automate strict PoLP enforcement.	ICSI implements a Privileged Access Management (PAM) or Privileged Identity Management (PIM) tool. Details of the same will be provided to the awarded Vendor.
28	Cybersecurity	II.n	...strictly governed by the Principle of Least Privilege (PoLP)...	Will a transition/discovery window (e.g., 45 to 60 days) be provided post-handover to audit existing user rights and establish a baseline before enforcing PoLP policies?	Immediate restriction of administrative privileges without a comprehensive baseline risk breaking legacy application dependencies.	The successful Vendor has to study all aspects of the environment after the issuance of the PO. The Vendor must carry out the assessment immediately from the start date of services.

29	Cybersecurity	II.n	...and that Multi-Factor Authentication (MFA) is enforced across all critical cloud and on-premises platforms.	Please provide a definitive list of all legacy applications, on-premises systems, and cloud portals that fall under "critical platforms" requiring MFA.	Legacy on-premises applications often lack native MFA integration support, requiring specialized authentication proxies.	Kindly refer to the scope of work and technical requirements specified in the tender document. Relevant details of the existing infrastructure / systems shall be shared with the successful bidder, wherever required, for the effective execution of services under the contract.
30	Cybersecurity	II.n	...Multi-Factor Authentication (MFA) is enforced...	Which corporate MFA solution provider (e.g., Microsoft Entra ID, Okta, Duo) is currently deployed at ICSI? Are the user access licenses for this MFA solution fully covered by ICSI?	Confirms compatibility requirements and ensures that user licensing costs are excluded from the vendor's commercial bid.	Kindly refer to the scope of work and technical requirements specified in the tender document. MFA established based on requirements of applications.
31	Cybersecurity	II.n	General Operational Clause Alignment	What are the minimal educational qualifications, cyber security certifications (e.g., CEH, Security+, CISSP), and experience levels required for the onsite FMS Engineers?	Directly impacts resource costing, wage projections, and commercial pricing model preparation.	As per RFP/Tender.
32	Cybersecurity	II.n	General Compliance and Environmental Risks	Are there any existing regulatory compliance mandates (e.g., CERT-In guidelines, ISO 27001) that the Service Provider's	Ensures that the designed cybersecurity framework meets explicit statutory and	Yes. The Service Provider shall strictly comply with all applicable regulatory mandates as suggested by ICSI Security Audit Team.

				security strategy must strictly align with?	government standard requirements.	
33	Earnest Money Deposit (EMD)	Clause 5	EMD forfeiture for withdrawal, refusal, or “any other unjustified reasons”	Kindly calrify if “any other unjustified reasons” would be limited to the examples provided to avoid arbitrary forfeiture.		As per the RFP / Tender
34	Extension	Annexure D-Clause 3	ICSI may extend contract for 3 years at its discretion	Please confirm whether extension requires bidder’s consent and renegotiation of commercial terms.		As per RFP/Tender.
35	Termination	Annexure D-Clause 4	ICSI right to terminate for cause. ICSI can terminate with one-month notice if there are more than 3 penalties in a month	The Service Provider requires a cure period of at least 30 days and an opportunity to make representations prior to termination for cause by ICSI. Further, we request that termination for cause be limited to “material breach” and “gross negligence” and that such rights be mutual in nature. These aspects may kindly be incorporated in the Agreement.		As per RFP/Tender.

36	Considera tion	Annexure D-Clause 5	Payment quarterly, inclusive of taxes	The interest on delayed payments should be applicable and the bidder shall have the right to suspend and/or termination of services in the event of prolonged non-payment. Further, kindly provide detailed timelines for payment of undisputed invoices and the process, resolution timelines, and clearance mechanism applicable to disputed invoices. These aspects may kindly be clearly incorporated in the Agreement.		As per RFP/Tender. Payment will be released as per the terms and conditions mentioned in the Purchase Order.
37	Refund of Performa nce Bank Guarantee	Clause –9 Security Deposit	No clarity on refund timeline post successful completion	Please clarify timeline for refund of Security Deposit and release of Bank Guarantee.		As per the RFP / Tender
38	Indemnity	Clause 23	Broad indemnity	We suggest that the indemnity obligations be expressly subject to the agreed limitation of liability cap and the exclusion of indirect or consequential damages. Further, it is recommended that indemnity be limited to actual, direct losses arising only from specific instances		As per RFP/Tender.

				such as wilful misconduct, fraud, gross negligence, third-party IPR infringement, and breach of applicable laws. These aspects may kindly be considered and incorporated in the Agreement at the pre-bid stage.		
39	Limitation of liability		Additional clause to be added in the SLA and RFP.	It is noted that the Agreement/RFP does not include a limitation of liability clause. In this regard, we suggest incorporating the following provision: "Notwithstanding anything to the contrary, the Service Provider's total aggregate liability, whether in contract, tort, or otherwise, arising out of or in connection with this Agreement, regardless of the form of action or theory of recovery, shall not exceed the total fees paid by ICSI in the preceding twelve (12) months under which the claim arises. In no event shall the Service		As per RFP/Tender.

				Provider be liable for any indirect or consequential damages, even if advised of the possibility of such damages.”		
40	Non-Solicitation		Additional clause to be added in the SLA and RFP.	It is noted that the Agreement/RFP does not include a non-solicitation clause. In this regard, we suggest incorporating the following provision: "During the term of this Agreement and twelve (12) months after the termination or expiry of the Agreement, neither Party shall solicit, offer work to, employ, or contract with, directly or indirectly, on its own behalf or through any other person or entity, any employees or consultant of		As per RFP/Tender.

				other Party or its affiliates. "		
41	Part 'A' - I. Instructions to Bidders	Clause 25 (Page 7)	"The FMS engineers must be on the payroll of the bidder for a minimum duration of one year (proof on the same must be submitted with the technical bid)."	Amendment Requested: Kindly relax this condition to allow resources who are lateral hires, provided they possess the required technical qualifications and total experience. The bidder will submit appointment letters/undertakings for such resources as proof.		As per RFP/Tender.
42	Part 'A' - I. Instructions to Bidders	Clause 25 (Page 7)	"Institute will do an interview with the FMS engineers before deploying them at site."	What is the turnaround time for ICSI to complete the interview process and provide clear feedback after the bidder submits resource profiles?	Necessary to ensure deployment timelines and avoid delay penalties.	ICSI shall complete the interview process and provide clear feedback (selected/rejected) within 7 working days from the date of submission of complete resource profiles by the successful bidder.

43	Part 'A' - II. Scope of Work	Clause b (Page 8)	"...take the Backup/Restoration of All Applications and Databases at Data Center... FMS Engineers must follow the Backup Policy and Data Synchronization as per policy."	Could ICSI share its established Data Backup and Synchronization Policy with bidders prior to final submission to understand data volumes and replication frequency?	Directly impacts the daily effort estimation of Level 3 administration tasks.	Will be provided to the awarded bidder.
44	Part 'A' - II. Scope of Work	Clause g (Page 9)	"Service Provider shall test the bandwidth on daily/weekly/quarterly basis and provide a report on the exact bandwidth provided by various ISP's."	Could you please confirm whether ICSI will provide the standard testing tools/ automated utilities required for bandwidth profiling, or if the vendor is expected to arrange and use their own testing scripts/software?	To ensure reporting alignment with ICSI's network expectations.	ICSI ISP has their Network Bandwidth Monitoring Web link sites. FMS can monitor the same and proactive alert monitoring system is established.
45	Part 'A' - II. Scope of Work	Clause h & i (Page 9-10)	"The FMS Engineers should be deputed at ICSI NOIDA Office to get KT (Knowledge Transfer) for 15 Working Days and all Cost... will be borne by the bidder." / "Backup FMS engineers... should visit the Institute office for (3) Three Working days in a month..."	Kindly clarify if the 15 days of Knowledge Transfer (KT) and the monthly 3-day backup synchronization visits for outstation engineers can be conducted virtually/remotely, subject to the availability of secure remote access (VPN, secure VDI, etc.).	Helps optimize administrative operational costs.	As per RFP/Tender.

46	Part 'A' - I. Instructions to Bidders	Clause 42 (Page 13)	"In case existing tools do not fulfil the purpose then new tools will have to be provided by the bidder. All the software/tool so supplied will be in the name of 'The Institute of Company Secretaries of India'."	As the requirement for enterprise-grade alternate monitoring tools may significantly impact the commercial bid, could ICSI please clarify the specific compliance gaps or limitations identified in the existing "Manage Engine OP Manager" solution?	Providing this clarity will enable all bidders to submit highly competitive and transparent commercial proposals.	The existing ManageEngine OpManager is the primary monitoring tool. The Vendor shall utilize it to the fullest extent. In case OpManager along with other available tools does not meet ICSI's requirements, the Vendor may propose suitable enterprise-grade alternate tools. Any such additional tools shall be supplied in the name of "The Institute of Company Secretaries of India". The cost of OpManager license shall be borne by the Vendor, while the cost of any additional approved tools shall be borne by ICSI with the sole discretion of the ICSI.
47	Part 'A' - I. Instructions to Bidders	Clause 39 - Penalty Terms (Page 13)	"In case there are more than 3 penalties on Service Provider in any month, the ICSI shall have right to terminate the contract by giving one month's notice..."	Kindly confirm, if an initial stabilization period (e.g., 60 days from project commencement) will be provided, during which SLAs are monitored for baseline tracking but penalties are waived to allow for system familiarization and process alignment.	Standard industry practice for infrastructure transitions to prevent premature default penalties.	As per RFP/Tender.

Sr. No	Page No.	Tender Clause/ Reference	Query/ Clarification Required	ICSI Reply
1	Page 19 / 20	Eligibility Criteria – Office establishment / representative at Delhi NCR, Mumbai, Kolkata, Chennai	We have our registered offices/ established presence at Delhi and Mumbai, and engineer presence at Chennai. We currently have more than 40 engineers deployed in Chennai across various projects and field support activities. We are fully capable of providing support at Chennai location. If we become successful / L1 bidder in this tender, we shall open an office at Chennai to fulfil the tender requirement and submit the required supporting documents. Kindly consider our request and allow participation based on our existing operational capability and undertaking for Chennai office establishment.	As per the RFP / Tender
2	Page 13	Software/ tools ownership	Apart from OP Manager, please confirm whether any other software renewal/ license renewal/ subscription renewal is required to be done by the service provider under this tender. If yes, kindly provide the complete list of such software/tools with name, version, quantity, current license status, renewal period and expected scope of bidder responsibility.	The Vendor has to bear the license cost of OpManager only.

3	Page 13	Monitoring Tools/ New Tool Requirement	The tender mentions that if existing tools do not fulfil the purpose, new tools will have to be provided by the bidder in the name of ICSI. Kindly clarify whether bidder should include cost for any additional monitoring/security/helpdesk/alerting tool in the commercial bid, or only OP Manager renewal/upgradation is to be considered.	The existing ManageEngine OpManager is the primary monitoring tool. The Vendor shall utilize it to the fullest extent. In case OpManager along with other available tools does not meet ICSI's requirements, the Vendor may propose suitable enterprise-grade alternate tools. Any such additional tools shall be supplied in the name of "The Institute of Company Secretaries of India". The cost of OpManager license shall be borne by the Vendor, while the cost of any additional approved tools shall be borne by ICSI with the sole discretion of the ICSI.
4	Page 23	OP Manager License Details	Kindly share the current OP Manager license details including edition, version, existing validity, support/AMC status, number of licensed devices, URL monitors, modules and whether upgrade from version 9.5 to latest version requires renewal only or fresh procurement.	Will be provided to the awarded bidder

5	Page 10 / 29	24x7 Monitoring Responsibility	The tender mentions 24x7 Data Centre/Network monitoring, while onsite engineer schedule is Monday to Saturday in two shifts. Kindly confirm whether 24x7 monitoring can be delivered through remote NOC/ centralized monitoring team after office hours, Sundays and holidays.	Yes, One Site FMS resource will Monitor/support as per office schedule and NOC team has to Monitor/support 24x7 through OP Manager tool and extend support time to time to on site FMS resources. However on site FMS resource must extend support through remotely after offie hours in case of any requirement time to time.
6	Page 8 / 9	Third-Party Vendor Dependency	The scope includes logging/forwarding calls to respective OEMs/vendors and submitting SLA violation reports. Kindly confirm that delay caused by OEM/ISP/third-party support vendors will not be treated as SLA violation of the FMS service provider, provided timely escalation and follow-up is done by the FMS team.	The FMS Service Provider shall be responsible for timely logging, coordination, escalation, and follow-up with the respective OEMs/ISPs/third-party support vendors. Delays attributable solely to OEMs/ISPs/third-party vendors shall not be considered as SLA violations of the FMS Service Provider, provided that the FMS team has performed timely escalation, regular follow-up, and maintained proper

				documentary evidence of such actions.
7	Page 10 / 28	Backup FMS Engineer Requirement – Quantity Clarification	The tender states that backup FMS engineers for both primary engineers should visit ICSI Noida office for 3 working days in a month, but the exact number of backup engineers required has not been clearly specified. Since backup support is normally required only when a primary engineer is unavailable, and it is unlikely that both primary engineers will be unavailable at the same time, one backup engineer may be sufficient to ensure service continuity. Kindly confirm whether one backup engineer will be acceptable, or whether ICSI specifically requires two separate backup engineers.	The requirement specified in the tender shall remain unchanged. The bidder is required to provide separate backup FMS engineers corresponding to the primary engineers to ensure uninterrupted support and continuity of services. Accordingly, provision of only one backup engineer shall not be acceptable, and two backup engineers are required as per the tender conditions.
8	Page 12 / 13 / 25	Rate Validity for 5-Year Contract	Tender mentions contract duration of 5 years, but payment terms mention rates quoted shall remain valid till 3 years from start date. Kindly clarify whether price escalation/revision will be allowed from 4th year onwards or whether rates quoted in financial bid will remain fixed for all 5 years.	The quotation shall be submitted strictly as per the Financial Bid format prescribed in the RFP. Further, under the payment terms clause, the validity period of the

				quoted rates shall be read as “5 years from the start date” instead of “3 years from the start date.”
9	Page 13 / 29	Penalty Applicability	Kindly clarify whether penalty will be applicable only for defaults directly attributable to the service provider, and not for cases dependent on ICSI approvals, OEM/vendor support, ISP downtime, force majeure, access delay, power/UPS failure or unavailability of required licenses/tools from ICSI.	Penalty shall be applicable only for deficiencies and defaults directly attributable to the Service Provider. Delays or service disruptions arising due to dependency on ICSI approvals, OEM/vendor support, ISP downtime, force majeure conditions, delay in access permissions, power/UPS failure, or non-availability of required licenses/tools from ICSI shall not be treated as SLA violations of the Service Provider, subject to proper reporting, escalation, and documentary evidence by the Service Provider.
10	Page 10 / 28	Cyber Security Responsibility	The scope includes cyber-attack prevention, vulnerability assessment, patching, MFA and incident response. Kindly clarify whether VAPT tools, EDR/XDR licenses, firewall licenses, MFA licenses, SIEM/SOC tools and security subscription renewals will	The cost of OpManager license shall be borne by the Vendor, while the cost of any additional approved tools shall be borne by ICSI.

			be provided by ICSI or are to be included in bidder's commercial scope.	
11	Page 23	Financial Bid Format – Additional FMS Engineer Cost	In the price bid format, provision has been given to quote the cost of additional FMS Engineers for Level 1, Level 2 and Level 3. However, as per the manpower requirement in the tender, onsite deployment is required for only two Chief FMS Engineers – Level 3. Kindly clarify the purpose of seeking additional rates for Level 1 and Level 2 engineers. Also, please confirm whether Level 1 / Level 2 engineers may be required in future under this contract, and if yes, kindly specify the expected role, location, working hours, qualification, experience and scope of work for such resources.	For future needs at any sites.

S.No	Page No	Clause No	Clause Description	Changes Requested / Clarifications	ICSI Reply
1	20	Annexure B2 Point No 4	The bidder should be a profit-making company for the immediately preceding Three (3) financial years and its net worth should be positive during this period.	Request to change the clause as below :-- The bidder should be a profit-making company for the immediately preceding **Two(2) financial years out of the last Three (3)** and its net worth should be	Same as per RFP/Tender.

				positive as on bid submission date.	
2	21	Annexure B2 Point No 15	The bidder must have adopted ITIL best practices and a valid ISO certification as on the date of submission of the bid ISO 9001:2008 /9001:2015 Equivalent certificate for quality and ISO 27001/ ISO 20005 Equivalent certificate for Data Security and Management. (Please attach supporting document).	Request to include the below two IT Service certification for good quality service. **ISO/IEC 20000-1:2018 -- IT Service Management System** **CMMI Services V3.0-Maturity Level–3** covering Infra Managed and Infra Life Cycle Services from CMMI Insitute and and should be verified by https://cmmiinstitute.com/learning/appraisals/results .	Same as per RFP/Tender.
3	23	PART 'C' (FINANCIAL BID)	(i) Renewal & Upgradation of current Tool: OP Manager (Current version 9.5 to Latest Version) Qty : 150 Devices + 5 URLs	Please share license details of last year renewal.	Will be provided to the awarded bidder
4	39	Annexure -F Point No 2	Number of ongoing FMS Contracts	Request to change the clause as below :--	Same as per RFP/Tender.

				Number of ongoing **FMS / AMC Contracts**	
5	12	II. SCOPE of Work: Point No 37	Payment Terms: FMS charges will be paid on quarterly basis at the end of each quarter for the preceding quarter	Request to change payment terms to **Monthly.**	Same as per RFP/Tender.