Annexure C

Corrigendum-II

Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center for ABP (Phase-III)-GFGNL in Gujarat

Issued by:
Gujarat Fibre Grid Network Limited
GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016/NOC

09th April 2025

Issued By:

Gujarat Fibre Grid Network Limited (GFGNL)

A Government of Gujarat Company

Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Corrigendum

The Bidders are requested to take note of the following changes made in the RFP document, which are to be considered while submitting the RFP response. They shall be presumed to have done so and submitted the RFP response / bid accordingly.

• This Corrigendum shall be the part of the RFP documents / process.

• All items specified in this Corrigendum supersede relevant items to that effect as provided in the original RFP documents. All other specifications, terms and conditions of the original RFP document shall remain unchanged.

• Text with strikethrough means it is deleted.

Fact sheet:

#	Particular	Details
9	Last date for submission of Bid/proposal	~~11/04/2025 at 06:10 pm~~ --→17/04/2025 at 6:10 pm

Pre-bid Query Response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1	46	System Overview	The system will streamline operations, ensure SLA compliance, and support end-to-end lifecycle automation with mobile-based deployment, GIS-based topology visualization, and OEM-	Plz clarify the meaning of Mobile based deployment? Does that mean, major modules of NMS/OSS/BSS shall be made available	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			engineer backed customization.	as a Mobile App??		
2	47	System Overview	• Comprehensive site deployment workflow with mobile-based features.	Does this mean one single MobileApp shall be made available for all the major modules of NMS/OSS/BSS??	-	Pls see revision
3	52	Mobile-Based Site Deployment & Readiness Workflow	The system must support a comprehensive mobile-based deployment process, including: • Engineer Assignment based on site location. • Map-Based Navigation for engineers to reach deployment sites. • Mobile App-Based Site Readiness Checks before deployment. • Mobile App-Based Site Inspection & Survey with automated validation. • Mobile App-Based Remote ATP (Acceptance Testing Procedure). • Pictorial Proof of Site Deployment and Signoff via the mobile app. • All site deployment workflows must be	Clarity is required on all the points mentioned in this section to be part of mobile app. Does site deployment means, software module deployment or hardware deployment?? or is it that one Mobile app shall be provided for each of these features??	-	As per the clause, to make virtual inspection effective and to reduce site visit by TPA or any other GFGNL authority, Mobile based verification is to be implemented. However Deployment workflow (major milestones like Site equipment up down, jitter, latency are to be flashed on dashboard. GFGNL may ask for customization of dashboard as per the designated authority requirement.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			centrally tracked on a Dashboard.			
4	37	API integration	Enable integration with SMS, email, and WhatsApp gateways for communication with field technicians/customers.	a. SMTP – EMAIL SERVER, SMPP for sms and Whatsapp subscriptions shall be provided by customer. Pls. Clarify and confirm.	-	Since Project monitoring and O&M of Fiber networks are to be with the help of GIS such facility shall provide cutting edge solu Subscription is to be provided by the System Integrator
5	125	6.1.11 DC/DR Sites	GFGNL will provide the space and power for DC site at Gandhinagar and DR site at Baroda or other city as per feasibility of GFGNL	Will GFGNL provide airconditioning/centralized cooling inside DC space. Pls. Clarify	-	Yes, GFGNL will provide sufficient air-conditioning/centralized cooling within the DC space as part of the infrastructure to ensure proper environmental conditions for all equipment.
6	-	6.2.7	Core Network & Cloud Infrastructure Design: This environment will host all the EMS of ABP PH-III OEM of both package. Physical infrastructure, including data center racks and cabling, SFPs, and not limited to this but all the require accessories will be designed	a. How many EMS systems are there for integrations including phase-1 , 2 and 3? b. Will they be co-located inside the same data centre? c. Will EMS systems be made available with their own racks,	-	Answer Given Inline: a. How many EMS systems are there for integrations including phase-1 , 2 and 3? Ans: We are looking for NMS which has ease in integration with EMS of standard products b. Will they be co-located inside the same data center? Ans:Yes, they will be collocated c. Will EMS systems be made available with their own racks, servers, storage and NW & security devices? Ans: EMS is not in this RFP Scope.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			and implemented by bidder at the SDC	servers,storage and NW & security devices? Pls. Clarify		
7	23	Table 2: Network Element (Indicative):	The total network elements = 101625 as per RFP	a. Is it the total number of Network elements to be monitored in all phases 1,2,&3. or this is only from phase 3. Pls. Clarify. b.If not, specify the network elements from phase-1 and phase-2 as well. c. To monitor all these network elements, are EMS systems already available ? If not , how many such elements to be interfaced direclty? Pls. Clarify	-	Ans Given Inline: a. Is it the total number of Network elements to be monitored in all phases 1,2,&3. or this is only from phase 3. Pls. Clarify. Ans: Since Ph 3 comprise all the GPs and nodes of PH-I and Ph-II. The element count given is total count. b.If not, specify the network elements from phase-1 and phase-2 as well. Ans: Already answered c. To monitor all these network elements, are EMS systems already available ? If not , how many such elements to be interfaced direclty? Pls. Clarify Ans: Pls refer ans of previous question

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
8	94	Backup and Replication Performance and SLA	Online/off-line data requirements have not been mentioned.	a. How many days online data required for each functionality/modules? Pls. Specify. b. what is the period for archiving the data (off-line) for each functionality/modules in tapes or disk backup? Pls. Specify.	-	a) Online data for each functionality/module should be retained for a minimum of 2year to meet operational, monitoring, and reporting requirements. b) Offline (archival) data for each functionality/module should be retained for a minimum of 10 years using suitable backup solutions (tape or disk). The detailed backup strategy will be finalized in consultation with GFGNL during project implementation.
9	94	Disaster Recovery Capabilities	The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency.	a. Is less than 5 sec RPO required only for critical data? Pls. Calrify. b. RTO hasnot been defined for DR of all application services. Pls. Specify.	-	a) Yes, the RPO of less than 5 seconds is specifically required for critical applications and data that are essential for continuous operations. For non-critical systems, standard RPO as per industry best practices will be acceptable and can be finalized during the implementation phase in consultation with GFGNL. b) The expected RTO (Recovery Time Objective) for critical application services is 30 minute. For non-critical application services, the RTO shall be finalized during the project execution phase based on business requirements and mutual agreement with GFGNL.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
10	-	System Overview	concurrent users expected for dashboard/reporting functions has not been mentioned.	How many concurrent users are expected for dashboard/reporting functions?No of alarms per second, No of trouble ticket per day, No of provisioning requests per day, Periodicity for performance data collection, any other dimensioning parameters Pls. Mention	-	How many concurrent users are expected for dashboard/reporting functions? Ans: Minimum 550 Users No of alarms per second, Ans: There should not be any limitation since critical alarm cannot be compromised. No of trouble ticket per day Ans:There should not be any limitation of TT/day also No of provisioning requests per day Ans: Unlimited, Periodicity for performance data collection, any other dimensioning parameters Ans: Since NOC is gathering the information from field, Periodicity is to be govern by the sender of the data and not the collector.
11	125	6.1.8 SLA-Based DCN Link Monitoring	The dimensioning and cost of DCN links connecting BharatNet EMS to S-NOCs (central/state) shall be considered. These links shall be SLA-based with penalties and monitored via the S-NOC.	Will GFGNL provide all links/MPLS/Internet links at Main and DR S-NOC sites and pay the monthly charges? Or Should this be arranged by SI/bidder? Pls. Clarify	-	GFGNL will be responsible for provisioning and bearing the cost of all required links, including MPLS, Internet links, and other necessary network connectivity at both the Main and DR S-NOC sites. The SI/bidder is not required to arrange or include the cost for these links in their proposal.
12	27	3.1.1	Eligibility Criteria - All the OEM Products including software components must have proven deployment and comissioning with five clients in this RFP in past 7 years.	This is a restrictive clause to indigenous OEM's, kindly relax number of clients to two.	-	Since GFGNL shall perform critical task of Project management of PH-III consisting of largest OFC network and huge number of active components, past relevant proven experience is mentioned. However for Make in India products, the relaxation in experience shall be applicable as per the MII policy. In lieu of relaxation in experience the provision of POC shall be applied

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
13	94	4.19	End point Protection of VMs	1. Scope of End point protection software installations - No. of VMs on which the software needs to be installed, VM's distinct Operating Systems (OS), Log retention period requirement. 2. Whether any specific requirement regarding hosting of solution - On premise/ Cloud based. Infrastructure requirement for Hosting the solution to be provisioned by Bidder or can be provided by client.	-	1. The endpoint protection software must be installed on approximately 150 VMs as per the indicative sizing mentioned in the RFP. The VMs will primarily run Linux (RHEL/CentOS/Ubuntu) and Windows Server operating systems. The log retention period required is 1 year for security monitoring and compliance purposes. 2. The endpoint protection solution is required to be hosted on-premises within the infrastructure proposed under this RFP. The bidder must provision the necessary infrastructure for hosting the solution as part of their scope.
14	4.19/ 1/94	Functional ity	End point protection software shall be single agent software for NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates.	**Change clause to below** End point protection software shall be single agent or dual agent from same OEM For NGAV, EDR, Threat Hunting, Application Control,	-	The requirement for a single agent solution is to ensure simplified operations, reduced overhead, and seamless management across all VMs. Hence, the original clause for a single agent solution will remain unchanged to meet operational efficiency and manageability objectives.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Vulnerability Protection, Firewall, and Device Control, operable without additional updates. Justification by Bidder: As there are multiple functioanlities asked in the Clause hence relaxing the clause from single agent to dualagent from same OEM as suggested will a low maximum participation		
15	4.3/2 /57	Interface & Performac e	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	**Change clause to below** The proposed appliance should have minimum of 8 x 1/10 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces	-	Pls see Revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				and appliances level. Justification by bidder: Changing the 8x1/10/25 Gigabit SFP+ Ports to 8x1/10 Gigabit SFP+ will relax the clause and will allow broader participitaion also as 4 Port 40/100 G gbps ports are asked hence 35 Gigabit will not have any usability in the solution		
16	4.3/2/57	Interface & Performace	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	**Change clause to below** The proposed single appliance should deliver **60 Gbps** of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 120Gbps on stacking supporting 72M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up	-	Please see acceptance in revision for wider participation and cost optimization/savings.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				to 120 Gbps throughput on stacking having <60 microsec latency JUstification by Bidder: As the Next gen firewall throughput asked in Thecnical specs section is 60 Gbps hence NIPS throughput must be inline to it also modifing the scalable throughput to 120 Gbps and 72 M Concurrent connections/second and maximum stacking TLS/SSL throughput to 120 Gbps will relax the clause and allow broader participitaion and removimg OEM Specific stacking functionality		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
17	4.3/3 /57	Functional ity	The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS.	**Change clause to below** The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS **or using endpoint tool ,Bidder can propose integration platform to achieve this functionality** Justification by Bidder: As STIX/TAXII are open platform and blocking may require integration	-	1. The acceptance of additionalities may restrict others. 2. The SI and potential OEM as good partner to GFGNL should provide additionalities printed on data sheets/web portal without cost to GFGNL as part of quality offerings optionally.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				with proposed endopoint solution hence intelligence sharing can happen via endpoint and NIPS integration than it will help to achieve the functionality and allowing broader participation		
18	4.3/3 /58	Functional ity	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality.	**Change clause to below** Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy or **have it own learning mechanism to understand network traffic pattern to create a baseling for anamoly an to shield vulnerabilities** Justification by Bidder: As NIPS itself have	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				signatures hence integration with third party vulnerbaility scanner is not always required hence changing this clause as suggested will relax the clause and allow broader participitaion thus removing OEM specific functionality		
19	63	4.6 Next Generation Firewall: Interface & Requirement	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports	The firewall should have minimum 4x100G **or 40G**, 8x10G or **25G** and **8 x1G** RJ45 interface from day 1 with fully populated SR transceivers as per the ports. **Also should have atleast 2 addational network I/O slots to add 2x100G or 4x40G/25G ports in future, depending upon organisation's choice.** Justification by Bidder: We are requesting this minor	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				modification to ensure cost efficiency while without any impact on the current and future scalability of Data Center Firewall.		
20	63	4.6 Next Generation Firewall: Performance Capacity	The Appliance must handle the threat prevention throughput of minimum 60 Gbps enabling security features and measured with Enterprise Mix / Application Mix traffic.	The appliance must support a minimum **50 Gbps** of threat prevention throughput with all security features enabled like Firewall, App Control, IPS, Anti-Malware/Anti-Virus. Justification by Bidder: This requirement is restricting broader vendor participation and limiting competition and cost-effective options. We request this minor modification to ensure wider participation and a more competitive procurement process while	-	We have specified dedicated items for specific purposes. The combined functionality in one or multiple boxes is allowed strictly in condition of combined performance including enablement of all purposes and all licenses without any cost to GFGNL. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device/devices are well established at individual and in totality as well. To derisk upon disqualification merely on ground of minor numeric values, a 10% tolerenace is allowed in general for product fitments in case of partipatary constraints in real sense and promoting wider partcipation. The illintend misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due deligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				maintaining security effectiveness.		
21	63	4.6 Next Generation Firewall: Performance Capacity	The Application should have Concurrent Sessions of – 60 million from day one.	The Application should have Concurrent Sessions of – 150 million from day one. Justification by Bidder: 60M concurrent sessions are too low comparing to new connections asked, considering minimum session duration of 120 sec it should be 120M, thus requesting you to amend the clause to make this	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				symetry and ensuring correct sizing parameter.		
22	64	4.6 Next Generation Firewall: Next Generation Firewall Features	NGFW solution should have the security features including IPS, Application control, Anti-Bot, DDOS prevention, Anti-Malware, Web filtering, DNS security, Sandboxing	NGFW solution should have the security features including IPS, Application control, Anti-Bot, DDOS prevention, Anti-Malware, Web filtering, DNS security/DNS Sinkholing. Justification by Bidder: Different OEM have different approach for DNS security, hence requesting this minor change without diluting functional requirement. Also we are requesting to remove sandboxing because sandbox is a separate solution available On-prem as well as a Service	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through. Further, in case of inclusion of sandboxing or some additional words for any OEM then same deemed optional for wider participation.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				but deteailed specs are not available in RFP. If sanboxing is required, please add the specifications or remove it.		
23	64	4.6 Next Generation Firewall: Threat Protection	Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV action such as allow, deny/drop, alert etc.	Should be able to perform Anti-virus/Anti-malware scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable action such as allow/allow after, discard/deny/drop, logging/alert etc. Justification by Bidder: Different OEM have different approach for handling virues/malwares threats hence requesting this minor change without diluting functional requirement	-	We have specified dedicated items for specific purposes. The combined functionality in one or multiple boxes is allowed strictly in condition of combined performance including enablement of all purposes and all licenses without any cost to GFGNL. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device/devices are well established at individual and in totality as well. To derisk upon disqualification merely on ground of minor numeric values, a 10% tolerance is allowed in general for product fitments in case of participatory constraints in real sense and promoting wider participation. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
24	64	4.6 Next Generation Firewall: Threat Protection	NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time.	Request to kindlly remove the clause. Justification by Bidder: This requirement is restricting broader vendor participation and limiting competition and cost-effective options, hence, we request to kindly remove the clause.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
25	64	4.6 Next Generation Firewall: Threat Protection	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.	Request to kindlly remove the clause. This requirement is restricting broader vendor participation and limiting competition and cost-effective options, hence, we request to kindly remove the clause.	-	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
26	65	4.6 Next Generation Firewall: Monitoring, Managem	Bidder to propose separate on-premises dedicated logging & reporting solution from same OEM (Virtual /Physical Appliance)	Bidder to propose separate on-premises dedicated Management, Logging & Reporting solution from same	-	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		ent and Reporting		OEM (Virtual /Physical) Justification: Different OEM have different deployment architecture, hence, requesting this minor change without diluting functional requirement.		
27	-	Next Generation Firewall: Support and Warranty	7+3 extendable years 24x7 comprehensive warranty from the OEM from day one	5 years extendable years 24x7 comprehensive warranty from the OEM from day one Justification : As technology is changing in every 3 years it is very hard to maintain the inventory for 10 years. We would request you to please change the warranty for 5 years.	-	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
28	126	6.1.15 Compliance w.r.t. DPDP Act. 2020	Bidder shall be responsible for establishes a framework to meet the compliance of DPDP Act 2020 or latest.	Bidder shall be responsible for establishing a framework to meet the compliance of DPDP Act 2020 or latest with atleast below parameters: As per the DPDP Act it is mandatory to have data security and awareness of data where it is hosted. We would suggest the solution must include a on-prem solution for 1500 users for data identification and mapping across GFGNL NOC environment, ensuring compliance and apply policies to ensure confidential data is shared only to authorized personals. Solution must have comprehensive list of pre-defined policies and templates with over 1500+ patterns,	-	GFGNL acknowledges the need for robust compliance with the Digital Personal Data Protection (DPDP) Act 2020 and related data security measures. However, GFGNL intends to keep the scope outcome-based and flexible to allow bidders to propose fit-for-purpose solutions. The bidder is responsible for implementing a framework that meets all relevant provisions of the DPDP Act 2020 (or latest), including data discovery, classification, protection, incident management, and necessary security controls. Bidders may incorporate additional advanced features (such as AI-driven insights, automated remediation, or policy templates) as part of their proposed architecture, subject to meeting the core compliance and governance objectives specified in the RFP.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				900+ True File type support, Hindi Language Support, Slow and low volume of data leakage protection, structured and unstructured fingerprinting, native encryption for removable media, Incident Risk Ranking and Unified Incident correlation and management for incidents across all the channels (Endpoint, Email, Web, Cloud apps etc.). Automated Discovery of data repositories to find shadow data & unprotected sensitive information including Enterprise GenAI solutions. AI-driven risk scoring to prioritize high-risk data exposure. Customized AI model training for		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				unique data needs. Automated remediation to restricting overexposed data & enforcing least privilege access. Redundant, Outdated, and Trivial (ROT) unstructured file analysis & Ransomware data exposure analysis. Data de-duplication to archive or delete files at risk. Task Manager functions for data custodians and owners. Persistent labeling for all scanned and classified files with DLP readable labels. Justification: We request this modification to align well with DPDPA requirements and addressing key data protection principles, security measures, and		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				compliance obligations.		
29	164	PART-A (Hardware & Software cost)	Next Generation Firewall - Qty (1+1)	Request you to kindly clarify the quantity, as in scope its mentioned that Both the sites	-	Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				(DC/DR) shall be in high availability mode. For DC - DR in HA it should be 2+2.		
30	46	4.1 Geographical Information System (GIS): 1 Hardware Requirements	User Licence requirement: For mobile GIS user, please consider the following User count for sizing purpose: •During Implementation phase •Concurrency: ~200 users •Total user Count: ~1125 •During O&M phase Concurrency: ~100 users •Total users Count: ~600	As per our understanding, the GIS application may require access for the back-office team to update the fiber inventory, visualize data, and extract reports from the PM tool and manage the operation & maintenance team.The required number of GIS software Web licenses is not specified. We kindly request GFGNL to specify the number of GIS Software Web users also to facilitate accurate hardware sizing.	-	Pls see Revision Tech Spec: Parameter No 20

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
31	30	3.2.1 Technical qualificati on criteria	2. Demonstration of prototype/readiness to meet technology led Governance in GIS a) Project management- b) Digital measurement book c) Virtual inspection	We kindly request GFGNL to add Fiber Inventory Management also. The clause should be a) Fiber Inventory Management b) Project management b) Digital measurement book c) Virtual inspection	-	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
32	52	4.2 Operation al Visibility Platform (NMS + OSS + BSS+ Network visibility):	7. Mobile-Based Site Deployment & Readiness Workflow The system must support a comprehensive mobile-based deployment process, including: •Engineer Assignment based on site location. •Map-Based Navigation for engineers to reach deployment sites. •Mobile App-Based Site Readiness Checks before deployment. •Mobile App-Based Site Inspection & Survey with automated validation. •Mobile App-Based Remote ATP (Acceptance Testing Procedure).	Mobile-Based Site Deployment & Readiness Workflow is a GIS-based operation and management usecase. We kindly request GFGNL to move the Mobile-Based Site Deployment & Readiness Workflow requirement from Clause 4.2, "Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):," to Clause 4.1, "Geographical Information System (GIS):"	-	Pls read revised clause as: The functionality of GIS in NMS related to mobile app section as raised in this query is removed. However, the mobile app limited to NMS purpose is included.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			•Pictorial Proof of Site Deployment and Signoff via the mobile app. •All site deployment workflows must be centrally tracked on a dashboard.			
33	124	6.1.1 Real-Time Data Access	The S-NOC will provide real-time operational status of OLTs/ONTs (GPs), Wi-Fi access points, FTTH connections, and more. This information will be accessible via web and app interfaces and integrated with the Digital Bharat Nidhi (DBN) Project Monitoring tool.	As per the clause we do understand that SNOC need to be integrated with Digital Bharat Nidhi, Project Monitoring tool. We want to understand wether DBN, PM tool is the existing deployed tool or it is also required to be BID in this tender ?	-	Project Monitoring tool is part of GIS Tech specs and need to procure however connectivity with C-NOC is to be done where bidder shall facilitate for integration

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
34	63	4.6 - Point no 2 (Interface & Requirement)	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports.	Please change to: "The firewall should have minimum 4 x100/40G,8x10G/25G and 8 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports." Justification: The proposed appliance supports aforementioned ports which are suitable for the requirement while also enabling flexibility for future network expansion as per requirement. Must for participation	-	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
35	63	4.6 - Point no 3 (Performance Capacity)	The Appliance should support minimum New Connections per Sec of 1 million.	Please change to: "The Appliance should support minimum New Connections per Sec of 1.5 million." Justification: With respect to the Threat prevention throughput requirement of 60 Gbps which includes all security features, it is recommended for appliance to have the capacity to support 1.5 million connections per second.	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
36	64	4.6 - Point no 3 (Performance Capacity)	The Application should have Concurrent Sessions of – 60 million from day one.	Please change to: " The Application should have Concurrent Sessions/connections of – 60 million from day one." Justification: We publish data on connections, not sessions. Hence the request to allow both terms. Required for participation	-	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
37	65	4.6 - Point no 8 (Authentication)	ISP WAN Link-Load balancing and Fail-over with Multiple Links, Application based load balancing, Fail-over based on parameters such as Latency, Jitter, Packet-Loss, QoS / Bandwidth management.	Please change to: " ISP WAN Link-Load balancing and Fail-over with Multiple Links, QoS / Bandwidth management." Justification: Requesting change as the mentioned updated specification are part of standard Firewall security features. Application based load balancing and fail over based on parameters parameters such as Latency, Jitter, Packet-Loss are features related to SD-WAN which is not relevant here & makes it OEM specific, hence requesting to remove from NGFW specifications.	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
38	66	4.6 - Point no 11 (Support, Warranty)	The NGFW should be proposed with 7 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live.	Please change to: " The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live."	Since the RFP specifications ask for appliance to be supplied with "comprehensive warranty and technical support for minimum 5 years", request to update the subscription licenses requirement also to 5 years to maintain uniformity.	Pl see revision in MAF
39	66	4.6 - Point no 11 (Support, Warranty)	7+3 extendable years 24x7 comprehensive warranty from the OEM from day one.	Please change to" 5+5 extendable years 24x7 comprehensive warranty from the OEM from day one with an option of hardware refresh after 5 years." Justification: In-line with ask for appliance warranty and subscription licenses, request to update the requirement for extendable warranty to 5+5	-	Pl see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				years. As the hardware has a lifecycle of generally 5-7 years due to technology obsolecence, bidder should allowed to refresh the Firewall hardware with same/better specs after initial 5 years & provide next 5 years of service		
40	57	4.3 - Point no 1 (Architecture)	The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution also proposed NIPS component should not use common firmware/underlying OS used for NGFW to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.	Please change to: "The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution" Justification: Please update the specification as requested, since the second part of the specification restricts participation & makes this OEM specific.	-	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
41	57	4.3 - Point no 2 (Interface & Performance)	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	Please change to: "The proposed appliance should have minimum of 8 x 1/10, 4 x 10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level." Justification: The proposed appliance supports aforementioned ports which are suitable for the requirement. The current clause is OEM specific & changes as suggested are required for other leading OEMs to participate. Must for participation	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
42	57	4.3 - Point no 2 (Interface & Performance)	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	Please change to: "The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput supporting 30M Concurrent Connections/Sessions having <2 microsec latency" Justification: The performance of NIPS is measured on the appliance IPS througput support and also latency. It is recommended to have latency less than 2 microseconds to avoid delay, and increasing the IPS throughput to 120 Gbps would provide better performance on the NIPS. The current clause is OEM specific & restricts participation & hence changes required	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
43	58	4.3 - Point no 3 (Functionality)	Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence having capability to trace action set to extract a private key from the network flow in order to help restore encrypted files to the victim while blocking traffic to the CnC server	Please change to: "Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence while blocking traffic to the CnC server" Justification: Please remove the part for extracting private key from the network flow to help restore encrypted files as it is a functionality of Endpoint Dtection & Response solution and not relevant to NIPS. Further the current clause is OEM specific & restricts participation & hence changes required	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
44	58	4.3 - Point no 3 (Functionality)	Should support 20,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, reconnaisance, identity theft etc.	Please change to: "Should support 15,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, rconnaisance, identity theft etc." Justification: 15000 IPS signatures exluding custom signatures is an ideal and holistic number to analyze all the traffic which will fall on the NIPS. The value needs to be modified to allow other leading OEMs to participate	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
45	58	4.3 - Point no 3 (Functionality)	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality	Please change to: " Should support VA scanners integration to fine tune the IPS policy or support an AI based threat intelligence to update and shield vulnerabilities automatically " Justification: As per increasing threat landscape, AI is being leveraged for launching cyber attacks by the attackers. While having integration with third party VA scanners is one way of achieving automatic fine tuning, having an AI based defence mechanism is the only successful technique to prevent such advanced attacks. Further the current clause is OEM specific & restricts participation & hence changes required	-	Repeated Query. Responded with intend of wider participation.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
46	58	4.3 - Point no 3 (Functionality)	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure	Please change to: "Should be a standalone dedicated NIPS appliance" Justification: This clause is specific to OEM and restrictive for participation. We request you to modify for wider participation and cost competitveness.	-	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
47	-	-	New Addition: 4.6 Next Generation Firewal	The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput having <2 microsec latency Justification: IPS is one of the primary features for Firewall, which is measured on two parameters, throughput and latency. It is recommended to have latency less than 2 microseconds to	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				avoid delay and throughput same as NIPS for better performance. The downstream NIPS is required to have IPS throughput of 10o Gbps & hence the NGFW must suuport IPS throughput much more than this value so that it does not belcome a roadblock		
48	-	-	New Addition: 4.6 Next Generation Firewal	Proposed NGFW should be of different make to the existing NGFW in NOC. Justification: It is recommended to have different OEM Firewall vendors on external and internal facing environment, to follow cyber security best practices as per guidelines.	-	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
49	-	-	New Addition: 4.6 Next Generation Firewal	The proposed firewall should not rely on proprietary ASICs and must be built on an open architecture utilizing multi-core CPUs to ensure protection and scalability against evolving security threats. If the proposed firewall leverages ASIC technology, its hardware performance must remain consistent even with the ASIC disabled. Justification: We request you to include this clause for open architecture based on Software and CPU capabilities so that flexibility, and cost competitiveness can be maintained.	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
50	page no 139 clause no 29	page no 139 clause no 29	The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement. Justification: As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	-	Pls refer specification of Link load balancer in tech spec 4.5/features wherein we have included following. which is reproduced herewith for reference. *"Appliance must have link load balancer license & server load balancer license comes by default along with base license including ipv6. Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, hash ip, target proximity and dynamic detect".* As part of the RFP, we are asking to run high performance applications including as mentioned in query. The Bidder is need to provide high performance and high availability architecture to keep system up all the time including peak load. And for that server load balancer functionality is to be provided by the bidder with all licenses related to SLB without any additional cost to GFGNL to achieve performance, scalability, fault tolerance, application availability of all these application like GIS, NMS, EMS,BSS and OSS.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
51	page no 141 section 6.5	page no 141 section 6.5	The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement. Justification: As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	-	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
52	page no 146 clause no 22	page no 146 clause no 22	Bidder has to ensure that the application to be deployed does not disrupt the operations and affect other GSDC & GFGNL infrastructure in terms of performance and security.	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement. Justification: As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	-	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
53	page no 139 clause no 29	page no 139 clause no 29	The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer Justification: A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other	-	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.		
54	page no 141 section 6.5	page no 141 section 6.5	The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer Justification: A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
55	page no 146 clause no 22	page no 146 clause no 22	Bidder has to ensure that the application to be deployed does not disrupt the operations and affect other GSDC & GFGNL infrastructure in terms of performance and security.	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer Justification: A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other	-	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.		
56	3.1.1 Eligibility Criteria | Pg. No. 27	3.1.1 Eligibility Criteria | Pg. No. 27	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined	We request to relaxed the network nodes and amend the criteria as below; The bidder should have experience in the successful execution of similar projects for the Central Government, any State Government, PSUs, Telecom, BFSI, or Public Listed Companies in India during the past five years from the date of bid submission, meeting the following criteria:	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	a) One project with a value of at least ₹40 crores with 3,000 network nodes, OR b) Two projects, each with a value of at least ₹30 crores with 2,000 network nodes, OR c) Three projects, each with a value of at least ₹20 crores with 1,000 network nodes. Justification: This will enable broader participation and encourage the mid size and emerging companies with relevant experience to participate		
57	3.1.1 Eligibility Criteria | Pg. No. 28	3.1.1 Eligibility Criteria | Pg. No. 28	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	CMMI Level 3 doesn't require for this kind of project. We request to remove this from list pls. Justification: Request for removal pls.	-	This seems suggestion of eliminating others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
58	6.1.11 DC/DR Sites | Scope of work	6.1.11 DC/DR Sites | Scope of work	The proposed solution should be implemented in DC & DR sites. GFGNL will provide the space and power for DC site at Gandhinagar and DR site at Baroda or other city as per feasibility of GFGNL.	We recommend that Disaster Recovery (DR) setup shall be implemented in a different Special Economic Zone (SEZ) or on a MeitY-empaneled cloud service provider's infrastructure, ensuring compliance with government regulations and security standards. Justification: Key benefits would be; Enhances Resilience – Using a different SEZ or cloud infrastructure ensures better geographical redundancy. MeitY Compliance – Ensures adherence to government security and data sovereignty guidelines. Flexibility for Implementation – Allows cloud-based	-	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				DR for scalability and faster recovery.		
59	3.1.1 Eligibility Criteria | Pg. No. 27	3.1.1 Eligibility Criteria | Pg. No. 27	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes	The captive project experience of a sister company or group company may be considered to meet the above-mentioned criteria. CA certificate may please be considered as supporting document pls. Justification: By amendment to this clause, it will create flexibility amongst bidders to participate smoothly.	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.			
60	4.6 - Point no 2 (Interface & Requirement), Pg. No. 63	4.6 - Point no 2 (Interface & Requirement), Pg. No. 63	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports.	Please change to: "The firewall should have minimum 4 x100/40G,8x10G/25G and 8 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports." Justification: The proposed appliance supports aforementioned ports which are suitable for the requirement while also enabling flexibility for future network expansion as per requirement.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Must for participation		
61	4.6 - Point no 3 (Performance Capacity), Pg. No. 63	4.6 - Point no 3 (Performance Capacity), Pg. No. 63	The Appliance should support minimum New Connections per Sec of 1 million.	Please change to: "The Appliance should support minimum New Connections per Sec of 1.5 million." Justification: With respect to the Threat prevention throughput requirement of 60 Gbps which includes all security features, it is recommended for appliance to have the capacity to support 1.5 million connections per second.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
62	4.6 - Point no 3 (Performance Capacity),	4.6 - Point no 3 (Performance Capacity), Pg. No. 64	The Application should have Concurrent Sessions of – 60 million from day one.	Please change to: " The Application should have Concurrent Sessions/connections of – 60 million from day one." Justification:	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
	Pg. No. 64			We publish data on connections, not sessions. Hence the request to allow both terms. Required for participation		
63	4.6 - Point no 8 (Authentication), Pg. No. 65	4.6 - Point no 8 (Authentication), Pg. No. 65	ISP WAN Link-Load balancing and Fail-over with Multiple Links, Application based load balancing, Fail-over based on parameters such as Latency, Jitter, Packet-Loss, QoS / Bandwidth management.	Please change to: " ISP WAN Link-Load balancing and Fail-over with Multiple Links, QoS / Bandwidth management." Justification: Requesting change as the mentioned updated specification are part of standard Firewall security features. Application based load balancing and fail over based on parameters parameters such as Latency, Jitter, Packet-Loss are features related to SD-WAN which is not relevant here & makes it OEM specific, hence requesting to	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				remove from NGFW specifications.		
64	4.6 - Point no 11 (Support, Warranty), Pg. No. 66	4.6 - Point no 11 (Support, Warranty), Pg. No. 66	The NGFW should be proposed with 7 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live.	Please change to: " The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live." Justification: Since the RFP specifications ask for appliance to be supplied with "comprehensive warranty and technical support	-	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				for minimum 5 years", request to update the subscription licenses requirement also to 5 years to maintain uniformity.		
65	4.6 - Point no 11 (Support, Warranty), Pg. No. 66	4.6 - Point no 11 (Support, Warranty), Pg. No. 66	7+3 extendable years 24x7 comprehensive warranty from the OEM from day one.	Please change to" 5+5 extendable years 24x7 comprehensive warranty from the OEM from day one with an option of hardware refresh after 5 years." Justification: In-line with ask for appliance warranty and subscription licenses, request to update the requirement for extendable warranty to 5+5 years. As the hardware has a lifecycle of generally 5-7 years due to technology obsolecence, bidder should allowed to refresh the Firewall	-	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				hardware with same/better specs after initial 5 years & provide next 5 years of service		
66	4.3 - Point no 1 (Architecture), Pg. No. 57	4.3 - Point no 1 (Architecture), Pg. No. 57	The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution also proposed NIPS component should not use common firmware/underlying OS used for NGFW to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.	Please change to: "The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution" Justification: Please update the specification as requested, since the second part of the specification restricts participation & makes this OEM specific.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
67	4.3 - Point no 2 (Interface & Performance), Pg. No. 57	4.3 - Point no 2 (Interface & Performance), Pg. No. 57	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	Please change to: "The proposed appliance should have minimum of 8 x 1/10, 4 x 10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level." Justification: The proposed appliance supports aforementioned ports which are suitable for the requirement. The current clause is OEM specific & changes as suggested are required for other leading OEMs to participate. Must for participation	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
68	4.3 - Point no 2 (Interface & Performance), Pg. No. 57	4.3 - Point no 2 (Interface & Performance), Pg. No. 57	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	Please change to: "The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput supporting 30M Concurrent Connections/Sessions having <2 microsec latency" Justification: The performance of NIPS is measured on the appliance IPS througput support and also latency. It is recommended to have latency less than 2 microseconds to avoid delay, and increasing the IPS throughput to 120 Gbps would provide better performance on the NIPS. The current clause is OEM specific & restricts participation & hence changes required	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
69	4.3 - Point no 3 (Functionality), Pg. No. 57	4.3 - Point no 3 (Functionality), Pg. No. 57	Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence having capability to trace action set to extract a private key from the network flow in order to help restore encrypted files to the victim while blocking traffic to the CnC server	Please change to: "Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence while blocking traffic to the CnC server" Justification: Please remove the part for extracting private key from the network flow to help restore encrypted files as it is a functionality of Endpoint Dtection & Response solution and not relevant to NIPS. Further the current clause is OEM specific & restricts participation & hence changes required	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
70	4.3 - Point no 3 (Functionality), Pg. No. 58	4.3 - Point no 3 (Functionality), Pg. No. 58	Should support 20,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, reconnaisance, identity theft etc.	Please change to: "Should support 15,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, rconnaisance, identity theft etc." Justification: 15000 IPS signatures exluding custom signatures is an ideal and holistic number to analyze all the traffic which will fall on the NIPS. The value needs to be modified to allow other leading OEMs to participate	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
71	4.3 - Point no 3 (Functionality), Pg. No. 58	4.3 - Point no 3 (Functionality), Pg. No. 58	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality	Please change to: " Should support VA scanners integration to fine tune the IPS policy or support an AI based threat intelligence to update and shield vulnerabilities automatically " Justification: As per increasing threat landscape, AI is being leveraged for launching cyber attacks by the attackers. While having integration with third party VA scanners is one way of achieving automatic fine tuning, having an AI based defence mechanism is the only successful technique to prevent such advanced attacks. Further the current clause is OEM specific & restricts participation & hence changes required	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
72	4.3 - Point no 3 (Functionality), Pg. No. 58	4.3 - Point no 3 (Functionality), Pg. No. 58	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure	Please change to: "Should be a standalone dedicated NIPS appliance" Justification: This clause is specific to OEM and restrictive for participation. We request you to modify for wider participation and cost competitveness.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
73	-	-	New Addition: 4.6 Next Generation Firewal	The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput having <2 microsec latency Justification: IPS is one of the primary features for Firewall, which is measured on two parameters, throughput and latency. It is recommended to have latency less than 2 microseconds to	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				avoid delay and throughput same as NIPS for better performance. The downstream NIPS is required to have IPS throughput of 10o Gbps & hence the NGFW must suuport IPS throughput much more than this value so that it does not belcome a roadblock		
74	-	-	New Addition: 4.6 Next Generation Firewal	Proposed NGFW should be of different make to the existing NGFW in NOC. Justification: It is recommended to have different OEM Firewall vendors on external and internal facing environment, to follow cyber security best practices as per guidelines.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
75	-	-	New Addition: 4.6 Next Generation Firewal	The proposed firewall should not rely on proprietary ASICs and must be built on an open architecture utilizing multi-core CPUs to ensure protection and scalability against evolving security threats. If the proposed firewall leverages ASIC technology, its hardware performance must remain consistent even with the ASIC disabled. Justification: We request you to include this clause for open architecture based on Software and CPU capabilities so that flexibility, and cost competitiveness can be maintained.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
76	26	3.1.1 Eligibility Criteria point no:2	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	**We request you to amend the clause as Below** The bidder must have a minimum average Annual Turnover of Rs. 100 crores during last three financial years 2021-22, 2022-23 & 2023-24, from the field/ business of **IT/ ICT/ ITES/networking & telecommunication.** Duly certified copies of the Balance sheets/Annual reports and a certificate from CA mentioning turn over from the respective field of business, for the last 3 FYs (2021-22, 2022-23 & 2023-24) are to be submitted as documentary proof	-	For wider participation- Pls see revision
77	26	3.1.1 Eligibility Criteria point no:2	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical	**We request you to amend the clause as** The bidder should have average annual turnover of	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March **2025.**		
78	29	3.2 Methodology of Selection BID EVALUATION PROCESS	The TENDERER will form a committee, which will evaluate the proposals submitted by the bidders for a detailed scrutiny. The evaluation will be based on QCBS (30:70) i.e., 30% weightage will be given to technical score and 70% weightage will be given to financial. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarificationvof their Proposals.	QCBS based Technical qualification criteria is not practised & followed in all Barathnet tenders Hence we request you to remove QCBS based Technical qualification criteria 30 marks for the bidders, In case the QCBS need to retained then the TENDEREER committee for evaluation should give a fair chance and seek	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				clarification from all the respective bidders.		
79	29	3.2 Methodology of Selection BID EVALUATION PROCESS & 3.3 Final Evaluation of Bid	The TENDERER will form a committee, which will evaluate the proposals submitted by the bidders for a detailed scrutiny. The evaluation will be based on QCBS (30:70) i.e., 30% weightage will be given to technical score and 70% weightage will be given to financial. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarificationvof their Proposals. Proposals will be ranked according to their combined technical (Tn) and financial (Fn) scores using the weights (T = 0.6 the weight given to the Technical Proposal; P = 0.4 the weight given to the Financial Proposal; T + P = 1).	Clause 3.2 Vs Clause 3.3 is contradicting on the weightage kindly clarify on the QCBS weightage that will be considered for evaluation	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
80	30	3.2 Methodology of Selection 3.2.1 Technical qualification criteria	3.2.1 Technical qualification criteria	The max marks calculation is equal to 110 which is greater than the total max marks i.e. 100. Kindly Clarify us with the revised distribution of marks	-	Pls see revision
81	30	3.2 Methodology of Selection 3.2.1 Technical qualification criteria point no:1	The bidder should have supplied, implemented and managed following projects in past 5 years. a)NOC (Network Operation Center)- 3 Marks b)Data center- 3 Marks c)NOC, Data center, (NMS/OSS or Network GIS)- 9 Marks Note: •The highest experience based will be given highest marks and there after rest will be given marks on percentile basis.	Kindly define Network GIS	-	Pls see revision
82	nil	New Query	New Query	We Request you to incorporate a consortium of two/three bidders, inclusion of a consortium will bring in more partners and a highly competitive	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				bid, and a win-win scenario		
83	63	4.6 - Point no 2 (Interface & Requirement)	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports.	Please change to: "The firewall should have minimum 4 x100/40G,8x10G/25G and 8 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports." Justification: The proposed appliance supports aforementioned ports which are suitable for the requirement while also enabling flexibility for future network expansion as per requirement. Must for participation	The proposed appliance supports aforementioned ports which are suitable for the requirement while also enabling flexibility for future network expansion as per requirement. Must for participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
84	63	4.6 - Point no 3 (Performance Capacity)	The Appliance should support minimum New Connections per Sec of 1 million.	Please change to: "The Appliance should support minimum New Connections per Sec of 1.5 million." Jusfication: With respect to the	With respect to the Threat prevention throughput requirement of 60 Gbps which includes all security features, it is recommended for appliance to have the	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Threat prevention throughput requirement of 60 Gbps which includes all security features, it is recommended for appliance to have the capacity to support 1.5 million connections per second.	capacity to support 1.5 million connections per second.	
85	64	4.6 - Point no 3 (Performance Capacity)	The Application should have Concurrent Sessions of – 60 million from day one.	Please change to: " The Application should have Concurrent Sessions/connections of – 60 million from day one." Justification: We publish data on connections, not sessions. Hence the request to allow both terms. Required for participation	We publish data on connections, not sessions. Hence the request to allow both terms. Required for participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
86	65	4.6 - Point no 8 (Authentication)	ISP WAN Link-Load balancing and Fail-over with Multiple Links, Application based load balancing, Fail-over based on parameters such as Latency, Jitter, Packet-Loss, QoS / Bandwidth management.	Please change to: " ISP WAN Link-Load balancing and Fail-over with Multiple Links, QoS / Bandwidth management." Justification: Requesting change as the mentioned updated specification are part of standard Firewall security features. Application based load balancing and fail over based on parameters parameters such as Latency, Jitter, Packet-Loss are features related to SD-WAN which is not relevant here & makes it OEM specific, hence requesting to remove from NGFW specifications.	Requesting change as the mentioned updated specification are part of standard Firewall security features. Application based load balancing and fail over based on parameters parameters such as Latency, Jitter, Packet-Loss are features related to SD-WAN which is not relevant here & makes it OEM specific, hence requesting to remove from NGFW specifications.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
87	66	4.6 - Point no 11 (Support, Warranty)	The NGFW should be proposed with 7 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live.	Please change to: " The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live."	Since the RFP specifications ask for appliance to be supplied with "comprehensive warranty and technical support for minimum 5 years", request to update the subscription licenses requirement also to 5 years to maintain uniformity.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
88	66	4.6 - Point no 11 (Support, Warranty)	7+3 extendable years 24x7 comprehensive warranty from the OEM from day one.	Please change to" 5+5 extendable years 24x7 comprehensive warranty from the OEM from day one with an option of hardware refresh after 5 years."	In-line with ask for appliance warranty and subscription licenses, request to update the requirement for extendable warranty to 5+5 years. As the hardware has a lifecycle of generally 5-7 years due to technology obsolecence, bidder should allowed to refresh the Firewall hardware with same/better specs after initial 5 years & provide next 5 years of service	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
89	57	4.3 - Point no 1 (Architecture)	The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution also proposed NIPS component should not use common firmware/underlying OS used for NGFW to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.	Please change to: "The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution"	Please update the specification as requested, since the second part of the specification restricts participation & makes this OEM specific.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
90	57	4.3 - Point no 2 (Interface & Performance)	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	Please change to: "The proposed appliance should have minimum of 8 x 1/10, 4 x 10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level."	The proposed appliance supports aforementioned ports which are suitable for the requirement. The current clause is OEM specific & changes as suggested are required for other leading OEMs to participate. Must for participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
91	57	4.3 - Point no 2 (Interface & Performance)	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	Please change to: "The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput supporting 30M Concurrent Connections/Sessions having <2 microsec latency"	The performance of NIPS is measured on the appliance IPS througput support and also latency. It is recommended to have latency less than 2 microseconds to avoid delay, and increasing the IPS throughput to 120 Gbps would provide better performance on the NIPS. The current clause is OEM specific & restricts participation & hence changes required	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
92	58	4.3 - Point no 3 (Functionality)	Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence having capability to trace action set to extract a private key from the network flow in order to help restore encrypted files to the victim while blocking traffic to the CnC server	Please change to: "Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence while blocking traffic to the CnC server"	Please remove the part for extracting private key from the network flow to help restore encrypted files as it is a functionality of Endpoint Dtection & Response solution and not relevant to NIPS. Further the current clause is OEM specific & restricts participation & hence changes required	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
93	58	4.3 - Point no 3 (Functionality)	Should support 20,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, reconnaisance, identity theft etc.	Please change to: "Should support 15,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, rconnaisance, identity theft etc."	15000 IPS signatures exluding custom signatures is an ideal and holistic number to analyze all the traffic which will fall on the NIPS. The value needs to be modified to allow other leading OEMs to participate	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
94	58	4.3 - Point no 3 (Functionality)	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality	Please change to: " Should support VA scanners integration to fine tune the IPS policy or support an AI based threat intelligence to update and shield vulnerabilities automatically "	As per increasing threat landscape, AI is being leveraged for launching cyber attacks by the attackers. While having integration with third party VA scanners is one way of achieving automatic fine tuning, having an AI based defence mechanism is the only successful technique to prevent such advanced attacks. Further the current clause is OEM specific & restricts participation & hence changes required	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
95	58	4.3 - Point no 3 (Functionality)	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure	Please change to: "Should be a standalone dedicated NIPS appliance"	This clause is specific to OEM and restrictive for participation. We request you to modify for wider participation and cost competitveness.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
96	-	-	New Addition: 4.6 Next Generation Firewal	The proposed appliance should deliver 120 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput having <2 microsec latency	IPS is one of the primary features for Firewall, which is measured on two parameters, throughput and latency. It is recommended to have latency less than 2 microseconds to avoid delay and throughput same as NIPS for better performance. The downstream NIPS is required to have IPS throughput of 10o Gbps & hence the NGFW must suuport IPS throughput much more than this value so that it does not belcome a roadblock	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
97	-	-	New Addition: 4.6 Next Generation Firewal	Proposed NGFW should be of different make to the existing NGFW in NOC.	It is recommended to have different OEM Firewall vendors on external and internal facing environment, to follow cyber security	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					best practices as per guidelines.	
98	-	-	New Addition: 4.6 Next Generation Firewal	The proposed firewall should not rely on proprietary ASICs and must be built on an open architecture utilizing multi-core CPUs to ensure protection and scalability against evolving security threats. If the proposed firewall leverages ASIC technology, its hardware performance must remain consistent even with the ASIC disabled.	We request you to include this clause for open architecture based on Software and CPU capabilities so that flexibility, and cost competitiveness can be maintained.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
99	83/204	Enterprise Storage, Platform	Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives.	Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD ~~NVMe~~ drives and spinning drives.	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	The requirement for tiering NVMe SSD and SAS/NL-SAS drives remains unchanged as per the RFP. The specified architecture is essential for ensuring high performance, scalability, and efficient storage management in the BharatNet Phase-III project. Mixing NVMe SSDs with SAS/NL-SAS drives in a single tier is a well-established practice for balancing performance and cost-efficiency, and it aligns with industry standards for large-scale network storage solutions.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
100	83/204	Enterprise Storage, Capacity & Scalability	Offered storage array shall be flexible on both Scale-up and Scaleout using array in-built firmware enabled clustering technology.	Offered storage array shall be flexible on Scale-up OR Scaleout using array in-built firmware enabled clustering technology.	Different OEMs have different methods of scaling for performance and capacity. The functional requirement of the RFP can be met by Data-in-Place upgrades as well. Mentioning both scale up and scale out restricts major OEM participation, hence request to modify.	GFGNL acknowledges the concern raised. The key requirement is to ensure that the offered storage array solution is flexible and scalable to meet both current and future capacity and performance demands. Therefore, the clause is modified as follows: Revised Clause: "Offered storage array shall be flexible on Scale-up OR Scale-out using array in-built firmware-enabled clustering technology." The solution should support either Scale-up (vertical scalability) or Scale-out (horizontal scalability) as per the OEM's architecture, provided it meets the overall functional, performance, and capacity objectives outlined in the RFP.
101	84/204	Enterprise Storage, Disk Drive Support and Encryption	Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives.	Offered Storage array shall support various capacities of ~~NVMe~~ flash and NL-SAS drives.	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
102	84/204	Enterprise Storage, Data Tiering	Offered Storage array shall be able to tier NVMe SSD and SAS/NLSAS Drives in a single po	Offered Storage array shall be able to tier ~~NVMe~~ SSD and SAS/NLSAS Drives in a single po	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
103	84/204	Enterprise Storage, Availability	Offered platform shall be configured in no single point of failureenvironment. Vendor shall design in such a way that storage layer shall provide 99.9999% data availability.	Offered platform shall be configured in no single point of failureenvironment. Vendor shall design in such a way that storage layer shall provide 99.999% data availability.	Current ask of 99.9999% availability is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	This is rural centric project , realted to multiple locations , multiple devices. The supervisor data is veru critical for monitoring purpose and taking action for high uptime. hence The requirement for 99.9999% data availability is a critical design criterion to ensure a highly reliable and resilient storage infrastructure for BharatNet Phase-III. This specification is aligned with industry best practices and is essential for maintaining uninterrupted operations and data integrity in a mission-critical environment.
104	84/204	Enterprise Storage, Integration VMWare Integration	Shall be certified for vVol based replication.	~~Shall be certified for vVol based replication.~~	Current ask of VVOL replication is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
105	86/204	Enterprise Storage, Snapshot / Point in time copy / Zero Copy	The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 500, total system should	The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	The specified limits for snapshots and clones are essential for scalability, data protection, and disaster recovery as per industry best practices. However for wider participation 10% tolerance is allowed.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Clone / Thin Clone	support at least 50,000 snapshots. Minimum 6 clone copies of each lun should be supported.	least 200, total system should support at least 20000 snapshots. Minimum 6 clone copies of each lun should be supported.		
106	86/204	Enterprise Storage, Remote Replication	~~The storage should support both Synchronous and Asynchronous Data Replication to remote site. The Storage should also capable of supporting 3-Way Disaster Recovery with Zero Data Loss Delta Resync.~~		Current ask is OEM specific. Request to delete to allow wider participation from leading OEMs.	The requirement for both Synchronous and Asynchronous Data Replication with 3-Way Disaster Recovery and Zero Data Loss Delta Resync is critical for high availability, business continuity, and disaster recovery in the NOC RFP. These features ensure data integrity and resilience in mission-critical environments. However, for wider participation the following principles are to be considered. 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
107	86/204	Enterprise Storage, Remote Replication	The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. Any external appliance if needed should be quoted to achieve this functionality.	The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. ~~Any external appliance if needed should be quoted to achieve this functionality.~~	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	The purpose is wider competition and therefore native/ external arrangement to fulfill the asked requirement is allowed without additional cost to GFGNL. The above option is to allow others to also participate without diluting overall objectivity and functionality for business continuity
108	86/204	Enterprise Storage, Data Loss	~~The solutions should ensure zero data loss (OEM need to provide assurance in the MAF)~~		Current ask is OEM specific. Request to delete to allow wider participation from leading OEMs.	Pls see revision
109	86/204	Backup Storage, Platform	Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives.	Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD ~~NVMe~~ drives and spinning drives.	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	The intent of the clause is to ensure a high-performance hybrid storage system capable of supporting both SSD (including NVMe) and traditional spinning drives to meet diverse performance and capacity requirements GFGNL will consider equivalent or better solutions that comply with the functional and performance goals specified in the RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
110	87/204	Backup Storage, Capacity & Scalability	Offered storage array shall be flexible on both Scale-up and Scaleout using array in-built firmware enabled clustering technology.	Offered storage array shall be flexible on Scale-up OR Scaleout using array in-built firmware enabled clustering technology.	Different OEMs have different methods of scaling for performance and capacity. The functional requirement of the RFP can be met by Data-in-Place upgrades as well. Mentioning both scale up and scale out restricts major OEM participation, hence request to modify.	We acknowledges the concern raised. The key requirement is to ensure that the offered storage array solution is flexible and scalable to meet both current and future capacity and performance demands. Therefore, the clause is modified as follows: Revised Clause: "Offered storage array shall be flexible on Scale-up OR Scale-out using array in-built firmware-enabled clustering technology." The solution should support either Scale-up (vertical scalability) or Scale-out (horizontal scalability) as per the OEM's architecture, provided it meets the overall functional, performance, and capacity objectives outlined in the RFP.
111	87/204	Backup Storage, Disk Drive Support	Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives.	Offered Storage array shall support various capacities of ~~NVMe~~ flash and NL-SAS drives.	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	This is performance related ask. The request of downgrading anything in terms of higher speed seems difficult to allow.
112	87/204	Backup Storage, Data Tiering	Offered Storage array shall be able to tier NVMe SSD and SAS/NLSAS Drives in a single po	Offered Storage array shall be able to tier ~~NVMe~~ SSD and SAS/NLSAS Drives in a single po	NVMe drives are high speed flash drives which do not function well with spinning drives. Request to modify as SSD drives to allow wider participation from leading OEMs.	Repeated query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
113	87/204	Backup Storage, Availability	Offered platform shall be configured in no single point of failureenvironment. Vendor shall design in such a way that storage layer shall provide 99.9999% data availability.	Offered platform shall be configured in no single point of failureenvironment. Vendor shall design in such a way that storage layer shall provide 99.999% data availability.	Current ask of 99.9999% availability is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	Repeated query
114	89/204	Backup Storage, Snapshot / Point in time copy / Zero Copy Clone / Thin Clone	The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 500, total system should support at least 50,000 snapshots. Minimum 6 clone copies of each lun should be supported.	The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 200, total system should support at least 20000 snapshots. Minimum 6 clone copies of each lun should be supported.	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	Repeated query
115	24	2.1	Logical Diagrams	What is NMAS? Are NMS-1, NMS-2,.. NMS-n already integrated with Phase 2 NMS? Is Proposed OSS shall be integrated with NMAS for Phase 2 and Phase 3 NMS/EMS?	Better understanding of the requirement	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				What is BMS? Is GIS shown in Logical digram is existing GIS in GFGNL Phase 3. If so, GIS asked in GFGNL Phase 3 shall be replace GFGNL Phase 2 GIS?		
116	26	3.1.1 (2)	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	The Bidder / OEM should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	Change Request	The Purpose of seeking financial strength is of bidder. The suggestion of qualifying bidder upon financial strength of OEM is mystifying advice.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
117	27	3.1.1 (4)	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	The Bidder / OEM should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of	Change Request	The Purpose of seeking financial strength is of bidder. The suggestion of qualifying bidder upon financial strength of OEM is mystifying advice.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.		
118	29	3.1.1 (9)	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	The Bidder / OEM must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	Change Request	This seems suggestion of eliminating others.
119	47	4.2 (1)	• Seamless new network deployments • Auto generation of configuration for new nodes and auto Integration. • Delta configuration	Our understanding is that, these requirement are associated with auto Network build and Provisioning on day 0. If so, these	Need clarity from OSS point of view	Pls read Tech spec 4.2 for EMS

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			updates for adjoining nodes. • SOP-based deployment for engineers with minimal skill requirements. • Comprehensive site deployment workflow with mobile-based features.	shall be done by using OEM's tool. Pl clarify		
120	48	4.2 (2)	Network Discovery, Network optimization & Inventory Management • Real-time bandwidth optimization across network segments.	What are the expected use cases for bandwidth optimization?	Better understanding of the requirement	Realtime BW optimization shall require to mitigate the congestion due to active and passive component failure and sudden requirement of BW spike. The solution should support necessary network configuration operations by administrator when needed.
121	48	4.2 (2)	Network Topology & Visualization • GIS-based topology diagrams with GIS integration.	Active Inventory shall be provided to GIS System & Topology shall be shown in GIS System. Is our understanding correct ?	Better understanding of the requirement	Understanding is correct
122	48	4.2 (2)	Network Topology & Visualization • Network path visualization: a time-correlated, unified view of all paths between any two points on network. With visibility across network, application, routing, and device layers.	Which application needs to be visualized? Pl clarify	Better understanding of the requirement	Application like GIS or NMS of other service provider

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
123	48	4.2 (2)	Network Topology & Visualization • The proposed solution should be able to clearly visualize the Hop-by-Hop visibility of the Underlay Network at a granular level Sub-Second) for Identifying clear problematic sections on the Glass pane view	What is meant by "granular level Sub-Second"? Pl clarify	Better understanding of the requirement	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
124	49	4.2 (2)	Deployment & Configuration Automation • Automated Deployment (AC): New nodes should be auto configured with minimal engineer intervention. • Delta Configuration Updates: Adjoining nodes should automatically receive delta configuration changes when new nodes are deployed. • SOP-Based Deployment: Engineers should only need to power up the device and connect cables. • Bulk Configuration Push: Network-wide	Our understanding is that, these requirement are associated with auto Network build and Provisioning on day 0. If so, these shall be done by using OEM's tool. Pl clarify	Need clarity from OSS point of view	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			configuration rollouts for standardization.			
125	49	4.2 (2)	Network Scanning The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	Our understanding is that, TWAMP server is available to monitor between GP to NOC or GP to Internet. Pl clarifiy	Better understanding of the requirement	The functional specification has been specified. It is the SI responsibility to provide the same
126	49	4.2 (2)	Network Scanning Automated fault, performance and security management reports	Are security management reports based on security logs received from router, switches, firewall?	Better understanding of the requirement	The functional specification has been specified. It is the SI responsibility to provide the same

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				As per our understanding, these reports are provided by Syslog Server.		
127	55	4.2 (23)	OSS tool should be certified TEC-GR-IT-NMS-003-01-NOV-15, comprehensive eTOM coverage	Compliance to TEC-GR-IT-NMS-003-01-NOV-15 to be provided or TEC certificate is required? Pl Clarify	Better understanding of the requirement	Both the standards are to be complied
128	118	5.41	Delivery Timeline	No mention of BSS in Delivery timelines. Pl clarify	Better understanding of the requirement	In Delivery Timeline Sr No-3 : NMS is combination of all the functionality of OSS+BSS. Same in Delivery Timeline Sr No 5 "demonstration of finished product" is also capturing the same
129	124	6.1.1	The S-NOC will provide real-time operational status of OLTs/ONTs (GPs), Wi-Fi access points, FTTH connections, and more. This information will be accessible via web and app interfaces and integrated with the Digital Bharat Nidhi (DBN) Project Monitoring tool.	Is it expected that NMS shall monitor Wi-Fi Access Points? If so, provide quantity	Better understanding of the requirement	Pls refer Table 2

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
130	133	6.4 (5)	Home broadband connectivity	Assumption: LCO's & MSOs will be customer to GFGNL and they take services from GFGNL to offer Home broadband connectivity service to the end customer. 1. Billing for the services taken by LCO's & MSO's will be done by Enterprise Billing System. 2. Billing for end customer is not expected to be done by Enterprise Billing System. How LCO's & MSOs end customer orders will be processed?	Better understanding of the requirement	LCOs & MSOs will act as GFGNL's customers and will procure services to offer broadband connectivity to end users. Billing for LCOs & MSOs will be handled through the Enterprise Billing System managed by GFGNL. End customer billing and order processing will be the responsibility of LCOs & MSOs, with no direct involvement of GFGNL in managing individual subscriber accounts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
131	141	6.5	The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC as shown in diagram	As per this, infra shall be provided by Bidder. Is this part of Delivery Milestone 3 "Demonstration of prototype/screen/ functional work flow of GIS and NMS as per RFP". Pl Clarify	Better understanding of the requirement	-Clarification: Yes, the bidder is responsible for developing and providing the platform for virtual inspection and user acceptance testing. The infrastructure required for hosting this application at S-NOC should be factored into the proposal. '-Relation to Milestone 3: The demonstration of the prototype/screens and functional workflow of GIS and NMS under Delivery Milestone 3 should include a preview of how the virtual inspection and acceptance testing platform will function. However, the full-fledged deployment and operational readiness of the platform will be required as per project timelines.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
132	3.1.1 Eligibility Criteria | Pg. No. 27	3.1.1 Eligibility Criteria | Pg. No. 27	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	This criteria carries the two different projects criteria we request to amend the criteria as; **1. Experience in Number of Similar Projects** **The bidder should have successfully executed similar projects for the Central Government, State Government, PSUs, Telecom, BFSI, or Public Listed Companies in India during the past five years from the bid submission date.** **The bidder must meet one of the following conditions:** **One project with at least 5,000 network nodes, or** **Two projects with at least 4,000 network nodes each, or** **Three projects with**	This will enable broader participation and encourage the mid size and emerging companies with relevant experience to participate	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				at least 3,000 network nodes each **OR** **Financial Qualification Based on Project Value: The bidder must have successfully executed projects meeting one of the following financial thresholds:** **One project with a minimum value of ₹40 crores, or** **Two projects with a minimum value of ₹30 crores each, or** **Three projects with a minimum value of ₹20 crores each**		
133	3.1.1 Eligibility Criteria | Pg. No. 28	3.1.1 Eligibility Criteria | Pg. No. 28	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	Here, CMMI Level 3 and above certification if non mandatory ask, we request to add weightage of CMMI Level 3 certificate in Scoring i.e. TQ .	-	Repeated query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
134	6.1.11 DC/DR Sites | Scope of work	6.1.11 DC/DR Sites | Scope of work	The proposed solution should be implemented in DC & DR sites. GFGNL will provide the space and power for DC site at Gandhinagar and DR site at Baroda or other city as per feasibility of GFGNL.	We recommend that Disaster Recovery (DR) setup shall be implemented in a different Special Economic Zone (SEZ) or on a MeitY-empaneled cloud service provider's infrastructure, ensuring compliance with government regulations and security standards.	-	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.
135	3.1.1 Eligibility Criteria | Pg. No. 27	3.1.1 Eligibility Criteria | Pg. No. 27	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each	The captive project experience of a sister or group company may be considered for meeting the specified criteria, with a CA certificate serving as a supporting document.	By amendment to this clause, it will create flexibility amongst bidders to participate smoothly.	Law of Land is implied. i.e.,The Company related act 1956/2013 in INDIA, partnership, hon'ble court orders and statutory authority related to mergers and acquisitions .

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.			
136	Clause No: 29, Pg. No. 139	Clause No: 29, Pg. No. 139	The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement.	As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
137	Section No: 6.5, Pg. No. 141	Section No: 6.5, Pg. No. 141	The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement.	As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	Repeated Query
138	Clause No: 22, Pg. No. 146	Clause No: 22, Pg. No. 146	Bidder has to ensure that the application to be deployed does not disrupt the operations and affect other GSDC & GFGNL infrastructure in terms of performance and security.	There is no server/application load balancer asked in RFP even though tenderer asked to host multiple application. And also asked to achieve certain level of performance along with service level of agreement.	As per RFP it is understood that tenderer asked to host multiple application including but not limited to GIS, NMS, EMS, BSS,OSS. To achieve performance, scalability, fault tolerance, application availibility of all these application Server/Application load balancer is recommanded.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
139	Clause No: 29, Pg. No. 139	Clause No: 29, Pg. No. 139	The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer 7.	A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
140	Section No: 6.5, Pg. No. 141	Section No: 6.5, Pg. No. 141	The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer 7.	A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
141	Clause No: 22, Pg. No. 146	Clause No: 22, Pg. No. 146	Bidder has to ensure that the application to be deployed does not disrupt the operations and affect other GSDC & GFGNL infrastructure in terms of performance and security.	RFP asked to develop and host multiple application like GIS, NMS, EMS, BSS,OSS however there is no mention of WAF(Web Application Firewall) in boq which is recommended to protect application at layer 7.	A Web Application Firewall (WAF) is essential for safeguarding applications against Layer 7 attacks. These attacks typically target the application layer, and a WAF helps defend against a range of threats, including OWASP Top 10 vulnerabilities, injection attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), bot attacks, scraping, credential stuffing, and other forms of automated threats. By filtering and monitoring HTTP traffic, a WAF can block malicious requests, ensuring that only legitimate users interact with the application and protecting it from various security risks.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
142	27	PQ / 3	The requirement specifies that The bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2024.	Request to quantify the networth to minimum Rs. 20 Crores in any three financial years out of last four financial years as on 31st March 2024.	Defining the net worth requirement in explicit monetary terms will encourage participation from financially stable and creditworthy companies, ensuring reliable and capable bidders.	It may limit the competition
143	28	PQ / 9	The Bidder must possess any three of the following certifications as on date of bid submission.	CMMI Level 3 or above certification is optional in PQ we request to make this requirement mandatory of include the score / marks in TQ for CMMI Level 3 or above certification.	For such esteemed project, carrying the CMMI Level 3 certification is highly critically. Companies with CMMI Level 3 certification have robust project management frameworks, leading to timely and efficient project execution.	Repeat Query
144	29	Bid Evaluation Process	The evaluation will be based on QCBS (30:70) i.e., 30% weightage will be given to technical score and 70% weightage will be given to financial.	We request clarification regarding The evaluation will be based on QCBS (70:30) i.e., 70% weightage will be given to technical score and 30% weightage will be given to financial.	We kindly request consideration for the following: Requesting to please confirm this is typo error; As QCBS as per scope required as 70% Tech & 30% Comm weightage.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
145	30	TQ / 1	The highest experience based will be given highest marks and there after rest will be given marks on percentile basis.	Kindly clarify that Bidder required to furnish Separate experiance to achieve marks as per TQ -1.	We kindly request consideration for the following: requesting to please ask for separate PO / Experience to get marks as per TQ 1 requirements.	Pls see revision
146	30	TQ	Not Asked / New Point	Request to include and add score/marks in TQ for Bidders cerification (ISO and CMMI Level 3 & above)	We kindly request consideration for the following: For Such project bidder's ISO and CMMI Certificate are highly critical.	The objective is wider participation and to meet overall purpose and solution.
147	30	TQ	110 Marks for TQ	Please make it 100 by adjusting the scope.	-	Pls see revision
148	33	Final Evaluation of Bid	The requirement specifies that ranked according to their combined technical (Tn) and financial (Fn) scores using the weights (T = 0.6 the weight given to the Technical Proposal; P = 0.4 the weight given to the Financial Proposal; T + P = 1)	Ranked according to their combined technical (Tn) and financial (Fn) scores using the weights (T = 0.7 the weight given to the Technical Proposal; P = 0.3 the weight given to the Financial Proposal; T + P = 1)	We kindly request consideration for the following: As QCBS is 70 : 30 Technical : Financial; Please Amend this.	Pls see revision
149	-	Warranty	The requirement specifies that 10 year (7 by OEM +3 extendable years by Bidder) 24x7 comprehensive warranty	Kindly Confirm that "Bidder required to factor only 7 Years Warranty OR 7 Years AMC Contract with OEM at the	We kindly request consideration for the following: Clerification only; As Some Part of bid asking for 10 Y warranty; kindly	Pls see revised MAF

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			from the server OEM from day one	time of supply. After 7Y GFGNL may renew the contract for next 3 Years.	confrim our understanding is inline as per RFP.	
150	108	Insurance / 5.20	The requirement specifies that Without limiting any of his other obligations or liabilities, the bidder shall, at his own expense, take and keep comprehensive insurance including third party risk for the plant, machinery, men, materials etc. brought to the site and for all the work during the execution and Operation & Maintenance.	We request clarification regarding Without limiting any of his other obligations or liabilities, the bidder shall, at his own expense, take and keep comprehensive insurance including third party risk for the plant, machinery, men, materials etc. brought to the site and for all the work during the execution period. and Operation & Maintenance.	We kindly request consideration for the following: After Invoicing the Material to GFGNL, the Material is part of GFGNL books. Bidder cann't take the insurance for this material. So please ristrict the insurance part on bidder till golive.	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services/Insurance against high payouts.
151	119	Note	The requirement specifies that CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value	We request clarification regarding CAMC (Comprehensive Annual Maintenance Contract) value for each year should	We kindly request consideration for the following: All Warranty asked 7Y from Day1; In Such Case it is not possible to offer min 7% as YoY AMC; So we request you to please make it 4%. Where the	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				not less than 4 % of CAPEX Value	capex to opex ratio is around 70:30 as per industry standard.	
152	125	6.1.11 DC/DR Sites	Both the sites shall be in high availability mode.	We seek clarification regarding the requirement for Data Center (DC) and Disaster Recovery (DR) in the High Availability (HA) setup. As per the Bill of Quantities (BOQ), our understanding is that identical resources are required at the DR site to match the DC setup. Kindly confirm if this interpretation is correct.	-	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.
153	125	6.1.11 DC/DR Sites	DC site at Gandhinagar and DR site at Baroda	We request clarification regarding DC site at Gandhinagar and DR site at different seismic zone than DC.	We kindly request consideration for the following: As per RFP both DC and DR in Same seismic Zone; So requesting to amend as per Global DC DR Guidelines.	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
154	126	6.1.14 / HOTO	Bidder shall take the HOTO of existing IT infra like Video wall, computer terminals and Non IT infra like furniture, UPS. AMC of the these infra shall be responsibility of the bidder. Information is given in Annexure B.		-	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
155	133	Service provisioning (Automated)	Proposed Solution shall comply Zero-touch provisioning for all type of services.	Kindly confirm that "Proposed Solution shall comply Zero-touch provisioning for all type of services. Where the 3PP HW is ZTP enabled and Competible with Bidder's Solution"	We kindly request consideration for the following: The Supply of Remore / Field Device is not part of NOC RFP; So if the 3PP device Supports ZTP & Compatible with supplied Solution by bidder under NOC RFP. Than only ZTP Possible from NoC Side.	Since GFGNL seeks such functionality from all the bidders of PH-III RFP and NOC-RFP as well as Back haul upgrade RFP. Solution shall be common.
156	136	Service Audit and Security compliance	Authentication of all the active devices in the network should be managed by a central authenticator, it should support role-based access, authentication, authorization and accountability capabilities.	To achieve this NAC and PAM Solution required.	We kindly request consideration for the following: The NAC and PIM-PAM is is not part of BOQ; So please add the same and also share min technical specifications for the same.	The AAA (Authentication, Authorization, and Accounting) server is required to authenticate NOC users securely, ensuring controlled access based on predefined roles and policies. The solution must support integration with multiple authentication methods, including LDAP, RADIUS, TACACS+, and multi-factor authentication (MFA), to enhance security. Additionally, audit logs should be maintained for compliance and monitoring purposes.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
157	148	6.8 Warranty Support	Warranty should not become void, if DST/GIL buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, thewarranty will not apply to such supplemental hardware items installed.	Request to removal of this project.	We kindly request consideration for the following: Major HW OEM Having policy to use only Certified options to add on capacity; any Component added which is not Certified / genuine lead to void the warranty.	Pls see revised MAF
158	161	7.11 VAPT	VAPT: Resolution / Remedy	We request clarification : if VAPT report suggest to add some additional Solution apart from the RFP BOM; The bidder required to only suggest the solution to GFGNL. And GFGNL will take it forward as out of Scope requirements.	We kindly request consideration for the following: As the Contract Period is here for 7 + 3 Years and Future vulnerabilities may required to purchse additional solution which is not part of current RFP.	1. The design of security architecture, supply of quality and reputed products for running the NOC in a secured manner is the prime responsibility of capable bidder. As part of the scope of work, we have indicated security products with high payouts to successful bidder for security compliances including quarterly VAPT for proactive and preventive measures in the larger interest of fulfillment of purpose of NOC. The bidders are advice to do proper due diligence while choosing security products. 2. It is expected that bidder shall design and implement security architecture and shall be expert to derive security strength of the product, writing scripts for preventions and ability to run and manage the underlaying network of Bharatnet and NOC components efficiently in most secured manner with best of security practices.
159	164	FINANCIAL BID FORMAT	PART-A (Hardware & Software cost)	We request clarification regarding Clerification : Please confrim the BOQ under Part A is required to setup at DC Site.	-	The understanding is correct

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
160	182	Annexure A Part 2 - Scope of Work as per BharatNet ABP RFP	Clarification	We request clarification regarding Kindly Confirm under this RFP bidder need to consider only scope Related to NOC (Central Infra + Manpower of NoC). There is no activity related to field services in the scope of bidder.	We kindly request consideration for the following: There are some activities in the RFP which is related to field services out side NOC; please confirm it's not SOW for NOC Bidder.	Field related activities shown in the annexure is for the reference for the bidders that support from software, module customization, template making and day in day out activities where field team are seeking help from NOC functionality prospective, need to be provided by bidder of this RFP
161	46	4.1 Geographical Information System (GIS): 1 Hardware Requirements	User Licence requirement: For mobile GIS user, please consider the following User count for sizing purpose: •During Implementation phase •Concurrency: ~200 users •Total user Count: ~1125 •During O&M phase Concurrency: ~100 users •Total users Count: ~600	As per our understanding, the GIS application may require access for the back-office team to update the fiber inventory, visualize data, and extract reports from the PM tool and manage the operation & maintenance team.The required number of GIS software Web licenses is not specified. We kindly request GFGNL to specify the number of GIS	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Software Web users also to facilitate accurate hardware sizing.		
162	30	3.2.1 Technical qualificati on criteria	2. Demonstration of prototype/readiness to meet technology led Governance in GIS a) Project management- b) Digital measurement book c) Virtual inspection	We kindly request GFGNL to add Fiber Inventory Management also. The clause should be a) Fiber Inventory Management b) Project management b) Digital measurement book c) Virtual inspection	-	Pls refer preceding response
163	52	4.2 Operation al Visibility Platform (NMS + OSS + BSS+ Network visibility):	7. Mobile-Based Site Deployment & Readiness Workflow The system must support a comprehensive mobile-based deployment process, including: •Engineer Assignment based on site location. •Map-Based Navigation for engineers to reach deployment sites.	Mobile-Based Site Deployment & Readiness Workflow is a GIS-based operation and management usecase. We kindly request GFGNL to move the Mobile-Based Site Deployment & Readiness Workflow requirement from	-	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			•Mobile App-Based Site Readiness Checks before deployment. •Mobile App-Based Site Inspection & Survey with automated validation. •Mobile App-Based Remote ATP (Acceptance Testing Procedure). •Pictorial Proof of Site Deployment and Signoff via the mobile app. •All site deployment workflows must be centrally tracked on a dashboard.	Clause 4.2, "Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):," to Clause 4.1, "Geographical Information System (GIS):"		
164	124	6.1.1 Real-Time Data Access	The S-NOC will provide real-time operational status of OLTs/ONTs (GPs), Wi-Fi access points, FTTH connections, and more. This information will be accessible via web and app interfaces and integrated with the Digital Bharat Nidhi (DBN) Project Monitoring tool.	As per the clause we do understand that SNOC need to be integrated with Digital Bharat Nidhi, Project Monitoring tool. We want to understand wether DBN, PM tool is the existing deployed tool or it is also required to be BID in this tender ?	-	Pls refer preceding response
165	94	Functionality/Point 1	End point protection software shall be single agent software for NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection,	**Change clause to below** End point protection software shall be single agent	As there are multiple functionalities asked in the Clause hence relaxing the clause from single agent to dual agent from same	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Firewall, and Device Control, operable without additional updates	or dual agent from same OEM For NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates.	OEM as suggested will allow maximum and broader participation	
166	57	Interface & Performance / Point 1	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	**Change clause to below** The proposed appliance should have minimum of 8 x 1/10 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	Changing the 8x1/10/25 Gigabit SFP+ Ports to 8x1/10 Gigabit SFP+ will relax the clause and will allow broader participitation also as 4 Port 40/100 G gbps ports are asked hence 35 Gigabit will not have any usability in the solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
167	57	Interface & Performance/Point 2	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	**Change clause to below** The proposed single appliance should deliver 40 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 60Gbps on stacking supporting 72M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 60 Gbps throughput on stacking having <60 microsec latency	As the Next gen firewall throughput asked in Technical specs section is 60 Gbps hence NIPS throughput must be inline and less to it i.e 40 Gbps also modifing the scalable throughput to 60 Gbps and 72 M Concurrent connections/second and maximum stacking TLS/SSL throughput to 60 Gbps will relax the clause and allow broader participitation and removing OEM Specific stacking functionality	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
168	57	Functionality / Point 2	The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in	**Change clause to below** The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs)	As STIX/TAXII are open platform and blocking may require integration with proposed endopoint solution hence intelligence sharing can happen via endpoint and NIPS integration still it will help to achieve the functionality and allowing broader participation	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			the NIPS.	to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS or using endpoint tool ,Bidder can propose integration platform to achieve this functionality		of work, functional aspects, supportive technical language for better understanding.
169	58	Functionality / Point 9	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality.	**Change clause to below** Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy or have it own learning mechanism to understand network traffic pattern to create a baseling for anamoly an to shield vulnerabilities	As NIPS itself have signatures hence integration with third party vulnerbaility scanner is not always required hence changing this clause as suggested will relax the clause and allow broader participitaion thus removing OEM specific functionality	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
170	21	2.1 Introduction	Project Background	Can you please confirm if the location phase-I & phase-II fiber is	-	Question is not clear

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				available and can be shared.		
171	24	-	Logical Diagrams	Can you please clarify if GIS Module will be required to integrate with NMAS module or multiple instances of NMS1, NMS2, NMS…n instances.	We are asking this question to understand how many active NMS instance integration will be required. Since different NMS can be from different vendors, it may need different technologies & interfaces for integration.	Here NMS1 , NMS2 denotes the terminals where operator use the NMS. Software shall be single. For concurrency pls refer revision
172	27	3.1.1. Eligibility Criteris	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project please refer the definition mentioned above .	Please clarify what is meant by "5 clients in this RFP". Do you mean 5 clients in Bharat Net past projects.	The componants mentioned in the Tchnical specifications	Pls see revision
173	27	3.1.1. Eligibility Criteris	The solutions of OEM must provide at least one reference case demonstrating GIS led support for more than 20,000 KM fiberization in any Government, PSU, pubic listed company or Telco- 5 Marks	This should also include "reputed private enterprise working for previous Bharat Net projects"	Reason for asking this question is that some of the large parties rolling out Bharat Net fiber are private companies and we have worked for them.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
174	30	3.1.1. Eligibility Criteris	Demonstration of prototype/readiness to meet technology led Governance in GIS a) Project management- b) Digital measurement book c) Virtual inspection	Please elaborate what is meant by Virtual inspection. Do you mean to say to review the execution work by reviewing the videography captured during the execution.	-	Yes, The understanding is correct
175	37	4.1 Base Map & Mapping Platform	The solution must bundle GIS layers for block boundaries, GP, and village locations. Additional necessary layers for network planning should also be provided.	We assume that "additional necessary layers" mean map layers of Road, Railway, Water and POIs. Please confirm. Are there any specific layers, please suggest.	-	As per RFP
176	37	4.1 Base Map & Mapping Platform	The solution should use a cloud-hosted map platform like Google Maps, supporting high-resolution satellite imagery, terrain view, and Streetview (where available).	Please mandate use of "Make In India" map layers	-	As per RFP
177	46	Hardware Requirements		You have mentioned concurrent Mobile GIS Users during project phase and O&M Phase. Can you please also suggest the	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				concurrent Browser based users,		
178	125	6.1.11 DC DR Site	Bidder shall plan DR as per the requirement of GFGNL for the critical applications or as per process.	Please suggest if DR site hardware configuration is to be planned at full load as main site or at a reduced load. Please specify the list of critical applications	-	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.
179	58	4.4 DDoS - Distributed Denial-of-Service/1	The proposed solution should be a dedicated solution as DDoS protection device, not as add on license Feature on ADC and NGFW.	Proposed appliance must be purpose built system and should be stateless technology not having any kind of state limitation such as TCP connections etc. Proposed appliance should be a dedicated appliance based solution (not a part of Router, UTM, Application Delivery Controller, IPS, Load Balancer,KVM , Proxy based architecture or any Stateful Device)	It is alsways recommended to have dedicated stateless ddos appliance to protect the security stack from state exaustion ddos attacks and shouldn't be part of any statefull devices like ADC,LLB UTM etc.Request you to ammend the clause as suggested for allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices and to avoid any tick mark solution getting quoted which will not help in protecting the	1. Both Stateful and stateless technology is allowed along with corresponding changes to meet functional and performance ask and objectivity. 2. We have specified dedicated items for specific purposes. The combined functionality in one or multiple boxes is allowed strictly in condition of combined performance including enablement of all purposes and all licenses without any cost to GFGNL. 3. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device/devices are well established at individual and in totality as well. 4.To derisk upon disqualification merely on ground of minor numeric values, a 10% tolerance is allowed in general for product fitments in case of participatory constraints in real sense and promoting wider participation. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					organisation from the complex ddos attacks.	do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
180	59	4.4 DDoS - Distributed Denial-of-Service/2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	System should support 16 x 10G SFP+ ports from day 1 . All the protection ports should support inbuilt Hardware and Software Bypass with Fail-Open and Fail-Closed options. No external bypass switch will be accepted.Dual Power supply. 4 TB or 1 year equalant logs should be kept on device / central management.Same appliance should support 4x100 G fibre bypass interfaces by replacing/upgrading NIC/Interfaces in future.	OEM specific clause and restricting the participation. This is not even practical to keep 4 TB storage on the appliance as every oem has its own different architecture. This specs seems to be supporting some KVM server not the Anti DDOS security appliance.Being fibre grid and the way technology or back plane keeps on changing , 100 G support in future is a must to have .Request you to ammend the clause as suggested for allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices.	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
181	59	4.4 DDoS - Distributed Denial-of-Service/3	Device should support at least 80Gbps throughput	System should have a Scalable Clean Throughput License approach for Legitimate Traffic. System should support Clean Throughput License Scalability upto 100 Gbps over next 5 years without changing the appliance.System should support Clean Throughput License of 20 Gbps from day 1 and scalability with a license upgrade.Proposed appliance should support more then 75 Million packet per seconds flood prevention rate on the same appliance. This performance figure must be mentioned in public facing datasheet.Should support latency less than 90 microseconds. Latency should be	The DDOS is sized on the basis of clean traffic throughput & flood prevention rate MPPS count where this provides scalable approach. These are calculated on the basis of the internet bandwidth and scalability.Request you to ammend the clause as suggested for a practical anti DDOS solution and fair participation of DDOS specific OEMs.	As per RFP. GFGNL has already specified throughput ask.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				documented in datasheet		
182	59	4.4 DDoS - Distributed Denial-of-Service/7	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack . System must be able to detect and mitigate Spoofed SYN Flood attacks and should support different mechanisms like: a) TCP Authentication b) TCP Out of Sequence Authentication c) HTTP Authentication - Redirect d) HTTP Authentication -	A lot of other functions are missing. Request you to ammend the clause as suggested as these are very common coutnermeasures of anti DDOS for layer 7	Repeated query. Responded with intend of wider participation at multiple places. Pl go through. The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				soft reset e) HTTP Authentication - JavaScript		
183	59	4.4 DDoS - Distributed Denial-of-Service/12	The solution should support Brute Force attack mitigation	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain atleas a million OEMs inhouse (no third party) IOCs to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a	A lot of other functions are missing. Request you to ammend the clause as suggested . Apart from brute force there are many other parameters.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				configurable interval.		
184	59	4.4 DDoS - Distributed Denial-of-Service/13	The solution should support the behaviour based DDOS mitigation.	The solution should support the host behaviour based DDOS mitigation using challenge response or http authentication	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
185	59	4.4 DDoS - Distributed Denial-of-Service/15	The traffic Auto learning threshold can be apply automatically after auto learning completed.	The traffic Auto learning threshold can be apply automatically or manually after auto learning completed.	OEM specific clause and in the production environment it is never recommended to apply auto threshold as that may hamper the production traffic with a single false positive. It has to be vet by the admin and then should be configured accordingly. Request you to ammend the clause as suggested for a fair competitivon and participation	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
186	59	4.4 DDoS - Distributed Denial-of-Service/17	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,OEM similar solution should be deployed and used by at least 4 Gov/PSU/BFSI customer in India to protect their own Core infrastructure from attacks and proposed solution should support native Integration with ISP clean pipe for preventing the volumetric flood. In case of volumetric flood on premise solution should send signal to the ISP Scrubbing centre for automated scrubbing at the ISP level . Auto signalling should be supported with atleast 4 Tier 1 ISPs Clean pipe services in India	Hybrid architecture is the main part while desising anti DDOS stretegy which is missing in the specification also proof of references are missing. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
187	59	4.4 DDoS - Distributed Denial-of-Service/18	The solution should support Access control list based on inbuilt GeoIP with configurable duration.	System should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown attacks without manual intervention. The system should not depend only on signatures for mitigation of DDoS attacks.It should restrict the IP address from specific segment like from TOR network and Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals	OEM specific clause and not a practical scnerio as if we block certain country traffic it should be blocked permanentnly. Also many other critical details are missing. Request you to change the clause as suggested for a fair competition and participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
188	59	4.4 DDoS - Distributed Denial-of-Service/19	The solution should able to import third party IP database through File or URL.	System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should act as gateway being at the extreme parimeter not allowing such malicious vectors to come inside the DC network.	OEM specific language also seems to be way old funciton. Todays scnerio every security device supports STIX TAXII same is used by CERTIN as well to automate the ingestions of IOCs in any device. DDOS protection being at the extreme parimeter should block such IOCs not only IPs at entry point itself.Request you to ammend the clause as suggested for next gen anti DDOS solution which should get integrated with CERTIN or any third party IOC provider.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
189	60	4.4 DDoS - Distributed Denial-of-Service/20	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP	Solutions should support Active - Active (High Availability) and Active - Passive Deployment. Solution should support inbuilt Fail-Open and Fail-Closed options for Hardware and Software Bypass	OEM specific and not a DDOS protection function as this feature contradicts the purpose of Anti DDOS solution. These are statefull devices feature where Anti DDOS is always recommended to be stateless else the device itself will become prone to the	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				feature on all inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment. No external bypass switch will be accepted.	DDOS attacks.Request you to ammend the clause as suggested for our participation.	
190	60	4.4 DDoS - Distributed Denial-of-Service/23	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	To be deleted	OEM specific and not a DDOS protection function as Anti DDOs is a transparent device and there is no routing on it is done. This seems some OEM is proposing LLB as a DDOS protection appliance. Requesst you to delete the clause as not relevent for any DDOS solution	We have specified dedicated items for specific purposes. The combined functionality in one or multiple boxes is allowed strictly in condition of combined performance including enablement of all purposes and all licenses without any cost to GFGNL. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device/devices are well established at individual and in totality as well. To derisk upon disqualification merely on ground of minor numeric values, a 10% tolerance is allowed in general for product fitments in case of participatory constraints in real sense and promoting wider participation. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
191	60	4.4 DDoS - Distributed Denial-of-Service/27	The solution shall provide the flexibility of performing configuration via GUI and command base remotely.	The system must have a dedicated management port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic. Proposed Appliance should have inbuilt GUI based monitoring, configuration management, diagnostics and reporting along with provision of Centralize management.	OEM specific language . The recommended architecture is having out of band management interface along with central management and a GUI on local device for configuration and monitoring.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
192	60	4.4 DDoS - Distributed Denial-of-Service/30	The solution shall support the provisioning of the reports - Attack reports - top sources, targets, attack type, Attack Severity Distribution, Attack Source Region	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region.The proposed OEM should have visibility of Tier 1 global ISPs Internet traffic to provide researched feeds of latest attack footprints to the appliance.	Missing other function related to the efficiency of research.Request you to ammend the clause as suggested.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
193	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must be able to generate summary attack report of daily/weekly/monthly	The solution must be able to generate summary attack report of daily/weekly/monthly. The proposed OEM should provide online portal access to get visibility of global attack trends along with yearly/half yearly reports on global attack trends for the team to define their	Missing other function related to the efficiency of research and reports which helps admin to take decisions on fine tuning the policies. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				stretegies for future.		
194	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must provide packet capture for debugging.	The solution must provide packet capture for debugging.The proposed solution should be certified for common criteria collaborative Protection Profile	Common criteria is a critical certification to identify the hardened OS of the system.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
195	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must support the generation of pdf reports containing the detailed statistics and graphs	The solution must support the generation of pdf reports containing the detailed statistics and graphs.Bidder must propose different OEM for the solution then WAF , IPS , SLB to create a multi layer security architecture.	Must to have clause to create multi layer security architecture as it is recommended to have multiple detection mechanism.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
196	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution must be on-premises and hardened as per GFGNL Information Security policy	Visibility platform/solution should have this essential feature.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
197	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution must have redundancy at all layer in both GFGNL datacenters .	Visibility platform/solution should have this essential feature.	As per RFP
198	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide health monitoring of virtual node, end point device for synthetic testing between selected site network and datacenters (Central system in DC/DR and agents on remote location)	Visibility platform/solution should have this essential feature.	Said requirement captured in Virtualization solution however GFGNL shall integrate the reporting functionality though monitoring to be done at separate platform which provide inherent role based of accessibility
199	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution must address and cover all aspects (front-end applications to back-end applications) of network service monitoring and able to decodes and drill down to session/transactions level	Visibility platform/solution should have this essential feature.	Pls refer the clause "4S" in Scope of Work.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
200	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. The solution should provide an end-to-end solution that includes Network Packet capture, Network Packet Broker, Network Performance Monitoring, end-user experience, voice, video monitoring and Synthetic monitoring as an Integrated solution.	Visibility platform/solution should have this essential feature.	Pls see functional requirement as specified in "4S"
201	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide support for passive and active monitoring of network traffic.	Visibility platform/solution should have this essential feature.	Pls see functional requirement as specified in "4S"
202	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should be able to monitor end-user network traffic via network devices and/or packet data at the datacenter without additional components / agent on the endpoint or server.	Visibility platform/solution should have this essential feature.	The requirement is NMS

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
203	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should be capable of performing suggestive analysis - based traffic anomaly to identify unusual or unexpected events and thresholds within the monitored environment.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP- parameter 13- SLA Monitoring & AI-Driven Analytics
204	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to baseline metrics and KPIs (Key Performance Indicators) in the monitored environment. Alert should be raised automatically to the respective team in case of any deviations to this baseline	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP- parameter 14 Reporting and Forensics/ analysis
205	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Should be able to monitor Internet access / activity in detail, even if the user is behind the proxy server	Visibility platform/solution should have this essential feature.	Functionality covered under BNG and NGFW

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
206	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Solution must support both IPv4 and IPv6 Protocols.	Visibility platform/solution should have this essential feature.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
207	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Solution should be able to monitor itself i.e., Monitor its health and send appropriate alerts to the system. SSD/HDD, Interface alerts etc.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP- parameter 17 -Configuration management
208	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	13. Solution must provide ability to backup and restore configuration files.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP- parameter 17 -Configuration management
209	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	14. Multi factor authentication / authentication with PIM	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP 20 -Security & Accounting Management
210	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	15. Packets/Logs must be stored in encrypted format & must be tamper proof	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP 20 -Security & Accounting Management

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
211	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	16. PCI- DSS: CHD / SAD related information must not be stored and displayed on user console /dashboard (as it will monitor unencrypted traffic)	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of Syslog and Server.
212	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	17. The network traffic capture include sensitive and confidential data within the application like user specific information (user name/password), confidential financial information, project information etc. The solution must note store such sensitive/confidential application content data to avoid any misuse by NOC/SOC engineer working on the solution. However, solution must	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of Syslog and Server.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				capture and store relevant information required for troubleshooting e.g. host information, session information, TCP values, errors/exceptions etc.		
213	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	18. Solution should be capable of performing real-time capture with following options for 24x7x365 network monitoring, advances protocol analysis, deep packet inspection:	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 1 -System Overview
214	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	19. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter- 18 Asset Management
215	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	20. The monitoring system must not use a "sampling" approach when collecting packets, which means it	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter- 10 Performance Management that comprehensive monitoring to be done.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				must collect & analyse all the packets to characterize data.		
216	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	23. Solution must provide packet analysis of both real-time and historic data. This should be capable of monitoring all conversations and able to analyze packet streams as defined below	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter- 10 Performance Management that comprehensive monitoring to be done.
217	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	24. Solution must provide intelligent deep packet capture and analysis capabilities for long-term storage and retrieval of network packets and statistics.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter- 10 Performance Management that KPI and deep analysis are to be done
218	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	25. Solution should be able to monitor various latencies/Response time involved in between client and server while accessing the application. For example - TCP RTT, Application	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter- 10 Performance Management that KPIs like Latency, Jitter and bandwidth to be measured

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				response time, Client connect time and server connect time etc.		
219	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	26. Solution must support addition customized network and applications protocols-based Monitoring on the TCP and IP stacks.	Visibility platform/solution should have this essential feature.	Question is not clear
220	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	27. Solution should be capable of decrypting SSL and TLS traffic with provided certificates and private keys	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of NGFW Parameter no- 5 Threat protection
221	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	28. Solution should be able to monitor peak active session for any application for any server (Where application is hosted) for any time duration along with the details of %age of successful transaction.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features since mission critical applications are not to be accessed
222	139	6.5 Operational Visibility Platform	Missing Critical functionality	29. Solution should be able to monitor errors if there are any and %age of	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features since mission critical applications are not to be accessed

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		failed transaction for any application for any server (Where application is hosted) for any time duration along with the details of error code messages for the same to get the root cause of that failure.		
223	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	30. Solution must provide deep packet inspection (DPI).	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
224	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	31. Solution should provide detailed packet decode and analysis for a wide range of industry standard protocols and applications, providing detailed decoding of web-based applications protocols, and services such those listed below:	Visibility platform/solution should have this essential feature.	Question is not clear
225	139	6.5 Operational Visibility Platform	Missing Critical functionality	32. Solution should be able to monitor wide range of well know applications	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features since mission critical applications are not to be accessed

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		along with the custom and home-grown application using packets and flows.		
226	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	33. Solution should be able to provide **in-depth monitoring of various databases and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
227	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	34. Solution should have in-depth monitoring for **front end application like HTTP, HTTPS and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
228	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	35. Solution should be able to monitor **Card Processing traffic and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
229	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	36. Solution should have in-depth monitoring for **MQ protocol (For example MSMQ, IBM MQ) and should have**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				dedicated monitor for the same:		
230	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	37. Solution should have **DNS monitoring** features **and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Said feature shall be covered in DDI
231	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	38. Solution should have **Active Directory, LDAP and Radius Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
232	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	39. Solution should have **DHCP Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Said feature shall be covered in DDI
233	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	40. Solution should have **Certificate Monitor and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
234	139	6.5 Operational Visibility	Missing Critical functionality	41. Solution should have **Unified communication**	Visibility platform/solution	Pls refer the clause "4S" in Scope of Work.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Platform (NMS + OSS + BSS):		environment monitoring **and should have dedicated monitor for the same:**	should have this essential feature.	
235	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	42. Solution should have **DHCP Monitor**ing and should have dedicated monitor for the same:	Visibility platform/solution should have this essential feature.	Response given in previous query
236	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	43. The network packet flow Switch should support Non Blocking Architecture	Visibility platform/solution should have this essential feature.	Question is not clear
237	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	44. Solution must provide central dashboard for network, application analysis. This must provide comprehensive high-level view of entire network thereby giving quick insight to resolve problems through the dashboard provided.	Visibility platform/solution should have this essential feature.	Response given in previous query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
238	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	45. Solution shall offer enterprise-wide visibility over the status of all the deployed components from a central dashboard. All the required licenses for analyzing the traffic (For ex- Web, DB, App, UC & Citrix) should be active from day one.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 1 -System Overview
239	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	46. Solution should be Hybrid in nature offering visibility across on-prim, public cloud, and private cloud from single/unified central management console	Visibility platform/solution should have this essential feature.	Response given in previous query
240	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	47. Solution should support traffic capture and analysis on Private Cloud (using virtual probe or third party vTAP), Containers, Dockers & other virtual Infrastructure. Virtual and physical network functions	Visibility platform/solution should have this essential feature.	Said requirement captured in Virtualization solution

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				in Private cloud environments as either a software agent within a multi-tenant Virtual Machine (VM) or a stand-alone, purpose-built VM. The solution must offer monitoring in a private cloud deployment using industry standard ecosystems.		
241	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	48. Solution should alert on the abnormal traffic behaviors such as whether there is a change in application traffic (sudden increases or decreases), drops in response time or if it disappears completely etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
242	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	49. Solution should be able to map traffic using IP address of individual host on the network, allowing for easy identification of individual host and	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- Network Discovery, Network optimization & Inventory Management in functional requirement of OVP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				associated traffic on the network. The solution should further be able to provide network packet flow diagram to illustrate network communication between multiple application tiers		
243	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	50. Solution must provide a central management console with probes / packet capturing devices being distributed across multiple geographical locations or public/private clouds.	Visibility platform/solution should have this essential feature.	At GFGNL, Multiple devices shall communicate with central management console through EMS.
244	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	51. Solution should be a complete for health monitoring and synthetic testing of application and network devices.	Visibility platform/solution should have this essential feature.	Response given in previous query
245	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	1. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	At GFGNL, Multiple devices shall communicate with central management console through EMS.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
246	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should be able to capture and **process 20 Gbps** (24x7x365 Capturing) of packet data in DC at real time with the average packet size of 800 - 1000 Byte	Visibility platform/solution should have this essential feature.	We have mentioned broad functional requirement
247	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should highlight network, application, and server hardware end infrastructures (including virtualized environment) and provide RCA (Root Cause Analysis).	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 1 -System Overview
248	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. This should provide back in time investigation & troubleshooting. The historical anaysis shall provide session analysis, host analysis, TCP analysys etc. for minimum period of last 7 days.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 10 Performance Management

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
249	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should have capability to store at least 12 months of high-level performance data, trend, issues, and events	Visibility platform/solution should have this essential feature.	There shall not be any limitation from OEM of solution to store the logs since storage is asked separately.
250	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Network packet Flow switch should have up to 48 line-rate ports (48 x1/10 GbE) and (6 x 40Gb)	Visibility platform/solution should have this essential feature.	Question is not clear
251	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. The Switch should be supplied with x. Nos – 1 GbE Copper SFPs x. Nos – 1 GbE MM Optics SFP x. Nos – 10 GbE MM Optics SPF+ x. Nos - 40 Gb trascivers Along with required Patch Cords	Visibility platform/solution should have this essential feature.	Question is not clear
252	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. The SNMP monitoring solution shall be sized for 10K devices/servers.	Visibility platform/solution should have this essential feature.	There is not limited to SNMP only . RFP has mentioned other protocols also with which competency to be matched. Device count also given separately.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
253	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. The synthetic monitoring shall be sized for 100 endpoints with atleast 20 end points testing concurrently.	Visibility platform/solution should have this essential feature.	We have mentioned broad functional requirement
254	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Comprehensive Solution that should have capability to capture packets from all zones defined in GFGNL datacenter network and end user system defined in scope of work	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 1 -System Overview
255	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. End to end solution is from the same vendor	Visibility platform/solution should have this essential feature.	GFGNL shall on board the system integrator to provide the functionality. GFGNL shall leverage the scope of SI with opening the possibilities of best performance.
256	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution is stiched with multi-vendor technologies	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP Parameter 1 -System Overview

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
257	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The proposed solution shall provide information of all the errors & its classification within the traffic on dashbaord. The dashboard showing error code distribution graph over time with classification of errors and numbers of errors in each category with ability to drill on any category or even single error.	Visibility platform/solution should have this essential feature.	GFGNL shall expect the customize dashboard as per the officer rank and requirement of stack holders
258	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. There would be multiple capture points within the network. The solution may aggregate the traffic. However, it shall maintain visibility of individual capture points. For e.g. if the same traffic is captured before and after firewall, the solution shall show status of the traffic at both captures	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				including time stamp to perform a hop by hop analysis or calculate latency/delay added in between.		
259	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Discover who and where traffic is routed in the Environment.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
260	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Discover delivery errors for the applications for which traffic is being captured.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
261	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Enable capture and storage of packet header information when only KPI calculations and data are required	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
262	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Enable or disable storing unnecessary user data traffic when required (packet truncation)	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
263	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Define and limiting packet sizes in the solution	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
264	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Capture the entire packet, Slicing the size of packet, Packet Truncation, Exclude specific packets and Capture only headers.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
265	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
266	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Correlation of the collated traffic data from different sources including synthetic testing agent	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
267	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	3. Confidential information & sensitive data with Application like User name, Password, Card No, PIN etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		must not be stored by the solution		
268	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
269	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. In event of GFGNL involving third party / OEM vendors for any troubleshooting activity and the need arising to share packet capture with them for the purpose of analysis, the solution shall be able to export such packet capture data which can be analysed using standard packet decode tool. However, without manual intervention, the solution shall ensure that the shared packet data	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				must not include entire application content data as is to avoid confidentiality issue or security breach.		
270	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Packet loss	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
271	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Retransmission rate	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
272	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Retransmission delay	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
273	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	4. Round trip time	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
274	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Throughput	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
275	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Traffic volume	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
276	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Number of connections	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
277	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Data transfer time	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
278	139	6.5 Operational Visibility	Missing Critical functionality	9. Server response time	Visibility platform/solution	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Platform (NMS + OSS + BSS):			should have this essential feature.	
279	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Delivery errors	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
280	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Web protocols: HTTP, HTTPS	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
281	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Core Services: SNMPv1-3, AD, DNS, DHCP, NTP, LDAP, FTP, SFTP, SMB v1/v2, SCP	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
282	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Email and Desktop: Secure POP3, Secure SMTP, IMAP, MS ActiveSync, NNTP_SSL, Notes, PoP3 etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
283	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Voice: SIP, H232, RTSP, RTP, SCCP	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
284	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Multimedia application: SIP, SIP Conference, SCCP, RTP, RTCP, MSRP and Video: H.323 etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
285	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Various MQ Protocols (MSMQ, IBM MQ Protocol etc.)	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
286	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Remote Desktop: Microsoft Remote Desktop, Citrix ICA, VMWare and Citrix Channel	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
287	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Along with Citrix ICA solution should support Citrix channel monitoring	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
288	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Database: Oracle DB, MySQL, Microsoft Access, DB2, DBASE, MSSQL, MSSQLMON, ORACLE_SRV, ORACLESQL, SQL_SRV, SQLNET	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
289	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Routing and others: Syslog, OSPF, BGP, IPsec, GRE	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
290	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility for latency , requests and failures for DB Connect, DB Query, DB Modification, DB Create/Drop.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
291	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide latency variation over time with database application usage. To get the idea of how latency varies if Usage (bps) varies for DB Connect, DB Query, DB	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Modification, DB Create/Drop.		
292	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
293	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failure %over time with total request, to get an idea on failure trend on database application.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
294	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code graph distribution for defined period for DB Connect, DB Query and DB Modification, to get a detailed idea on error message which are getting generated in	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				between specific client-Server communication transaction.		
295	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide error code distribution for certain period for GET, PUT and POST, to get a detailed idea on error message which are getting generated in between specific client-Server communication.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
296	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Should provide visibility for latency, requests and failures for GET, HEAD and PUT/POST	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
297	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide latency variation over time with application usage. To get the idea of how latency varies if application usage varies	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
298	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
299	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide failure %over time with total request, to get an idea on failure trend	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
300	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Should provide visibility for Latency, Requests and Failures for MQ Messages for example open/close, put/get and Put 1.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
301	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Solution should provide latency variation over time with application usage. To get the idea of how latency varies if application usage vary.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
302	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
303	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Solution should provide failure %over time with total request, to get an idea on failure trend and also should know which message (open/close, put/get and Put 1) is faling and the reson of the failure.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
304	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Solution should provide error code distribution for certain period for open/close, put/get and Put 1, To get a detailed idea on error message which are getting generated in between specific	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				client-Server communication.		
305	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility for A-AAAA, PTR-NAPTR and PUT/POST queries.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
306	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide latency Variation over time with DNS application usage. It will give idea of how latency varies if DNS query varies	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
307	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with DNS application latency if any	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
308	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	4. Solution should provide DNS application failures overview for	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		accessing the DNS application health		
309	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for A-AAAA, PTR-NAPTR and SRV, to get a detailed idea on error message which are getting generated in between specific client-Server communication transaction	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
310	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Ability to give latency, requests and failures for Authentication, Search & Compare, Modify and Others.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
311	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for Authentication, Modify etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
312	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency).	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
313	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with total requests, gives idea on failure trend and which are being failed for ex: Authentication, modify etc. and transaction count with %Failed.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
314	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Error code distribution gives detailed error message which is getting generated in between specific client-Server communication with error code count with failed transaction.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
315	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	a) Ability to give latency, requests and failures for DISCOVER,	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		REQUEST, RENEW and Other		
316	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for DISCOVER, REQUEST, RENEW etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
317	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency)	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
318	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with requests, gives idea on failure trend and which are being failed, for example DISCOVER, REQUEST, RENEW and requests with %Failed	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
319	139	6.5 Operational Visibility Platform	Missing Critical functionality	e) Error code distribution, gives detailed error message which is	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		getting generated in between specific client-Server communication with error code count with failed transaction		
320	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility on the certificates which are installed on the specific servers.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
321	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. It should also provide visibility whether certificate is self-signed, or third party signed certificate.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
322	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Certificate monitoring should provide server Name along with count of certificate with details of certificate for example if certificate is ok, if there are any warning or in critical stage.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
323	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. It should also provide us expiry days for certificate.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
324	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide functionalities of setting alerts for the certificate expiry days.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
325	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility in unified communication user plane (SIP etc.) protocol as well as data plane (media - RTP, RTCP etc.) protocols	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
326	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution Should provide visibility for latency, requests and failures in Registration and Call Setup	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
327	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		idea on performance of number of requests affected with application latency.		
328	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failures over time with total calls, to get an idea on failure trend on session related protocols.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
329	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for call registration and Call setup, to get a detailed information on error messages which are getting generated in between specific node and unified communication server.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
330	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide detailed session analysis for user plane protocol to get detailed information (for	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				example - server name, client name, calling party, called party, CODEC, Avg RT (ms), Start Time, Duration with status) for troubleshooting purposes.		
331	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should provide visibility on network problem in Unified Communication (i.e. Audio Video packets) like Packet Loss, Jitter, Round Trip Delay and packets Out of Sequence along with stream counters over time to monitor QoS Mismatch.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
332	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should provide detailed information about source and destination (For example - QoS, Codec, SSRC, Packet loss and Jitter	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
333	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to provide issues in between called party and calling party with the details like Packet loss, Voice Jitter, Voice Pkt Loss and also solution should provide media Streams details like Average active, Completed and deviation from QoS	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
334	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Solution should provide call search option based on IP address and Extension to search the specific call to troubleshoot the issues in between called party and calling party.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
335	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution shall be able to instrument packet in private cloud like VMWare, VMWare NSX, HyperV, Open Stack etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
336	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The solution shall also be able to instrument packets in container, docker and Kubernetiv environement.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
337	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution shall also be able to instrument packets in public cloud like AWS, Azure, Oracle, Google, IBM Softlayer etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
338	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The solution shall be able to understand and work in SDN environments like Cisco ACI, VMWARE VxLAN etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
339	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support VDI (Microsoft, VMware, Citrix etc.) to identify and triage network performance issues impacting VDI based services and identify the root cause of problems. Solution should be able to obtain visibility of VDI infra, including	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				remote access, client, virtualization, Web, front-end, application, and associated database.		
340	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The Packet Flow shall support - aggregation (Fully flexible any-to-any port mapping) - replication, - filtering, - load balancing, and - source port tagging	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
341	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The network packet Flow switch should be monitored via Syslog/SNMP	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
342	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The Packet Flow Switch should have redundant, hot-swappable power supplies and Fan Module.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
343	139	6.5 Operational Visibility Platform	Missing Critical functionality	4. Monitor Traffic Port Tagging Should Provides identification of	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		traffic based on source network/link using VLAN tagging		
344	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Local and Remote Management - graphical interfaces - CLI - Alerts can be received by any Syslog server or SNMP manager	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
345	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must include a comprehensive logging capability to log all the system events and the solution must be able to send the system logs to SIEM /syslog servers and also should be able to send SNMP trap to the SNMP trap receiver system.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
346	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support integration with Email to receive the alerts on the email.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
347	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must be able to perform time synchronization with NTP server	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
348	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support integration with Auto ticket logging (ServiceNow)	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
349	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support integration with SIEM (ARCSIGHT)	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
350	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should support integration with TACACS (Cisco ISE) /PIM (ARCON) for device management for MFA	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
351	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should be integrated with SOC, NoC IToM environment.	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP 23 -Standards

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
352	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should work seamlessly with all industry standards Data center Software defined network e.g., Cisco ACI for data center infra, SD-WAN, SD-LAN and similar technologies	Visibility platform/solution should have this essential feature.	We have mentioned broad functional as well as integrational requirements
353	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Features capturing packets from various WAN appliances	Visibility platform/solution should have this essential feature.	The requirement is NMS
354	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Supports TAP	Visibility platform/solution should have this essential feature.	The requirement is NMS
355	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The dashboard should be able to provide different widgets for different components as online analysis to automatically identify which widget/component or tier is	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				contributing to slowness of the monitored transaction.		
356	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Dashboard should be able to show captured traffic for monitoring individual traffic type or applications based on Packet Size or Application type.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
357	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The dashboard should show relevant performance or error messages within the captured packets that are associated with problems for root-cause analysis.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
358	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Dashboard should have analytical capabilities for assisting in identifying the root cause through a multitude of dashboards and	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				reports. The solution should also simplify the operations monitoring process significantly by helping define the correct team to address the problem. e.g., network, application, server, middleware or database teams. The objective is to reduce Mean Time to Identify (MTTI) and Mean Time to Resolve (MTTR)		
359	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Dashboard must include an interactive user interface that allows users to view real-time & historical analysis, flows end-to-end that includes hop-by-hop traffic analytics at each capture point in the flow	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
360	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Dashboard should be able to provide usage of multiple dimensions such as network, application, voice and video together on dashboard	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
361	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Dashboard should provide real-time monitoring of all traffic being sent from and received to Data center. The monitoring should include parameter such as response times, usage pattern etc. for identifying communication issues between user and application servers.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
362	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Dashboard must provide an analysis of the condition or health of the network. It should be able to measure counts and response times for every network transaction captured in the Data Centers.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
363	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Dashboard shall provide key metrics for health measurement will be like application and link throughput volume, retransmissions, success/fail transactions, and application error codes.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
364	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Metrics must be presented on a summary panel with chart details, allowing the user to quickly gain insight into the behavior of multiple applications across multiple segments	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
365	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Dashboard should be able to provide complete visibility of network activities, end user experience, and application traffic and network performance. It must also provide summarized analysis, breaking down application	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				response time into following components: a) Client/Server response b) Network bandwidth c) Network latency d) Network congestion e) Network protocol (e.g., TCP)		
366	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Dashboard should provide information to identify and isolate to determine whether end-user experience of slowness in accessing of the information is due to a network or an application issue. It should be able to calculate response times for all relevant applications and determine the impact on user experience.	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
367	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	13. Solution should be able to detect and alert on network congestion incidents with the ability to drill into client, server, application, or user levels to identify the root cause of the problem. It should be further able to measure traffic by user or application, identify bandwidth hogs and provide information about sites/URLs which are being consumed. The solution must be able to identify the root cause of the problem by pinpointing on the entity in question.	Visibility platform/solution should have this essential feature.	The requirement is NMS
368	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	14. Solution must be able to provide network traffic monitoring and forensics. It should be able to furnish summarized Executive Dashboard and	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				detail traffic analysis dashboard which gives customizable views of network traffic, allowing the user to spot potential problems quickly with top ten views of network traffic data. It should give the root cause of bandwidth issues with an intuitive point-and-click interface		
369	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	15. Dashboard configuration should not be limited to pre-defined templates and should be dynamic. There should not be any license limitation on creation of the dashboards in the monitoring system	Visibility platform/solution should have this essential feature.	As per the OVP technical specification Dashboard requirement is meticulously defined and weightage of the same is reflecting in technical qualification of product with PoC. Bidders is invited to arrive with the innovative and informative dashboard with asked parameters but not limited to the same.
370	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should offer an integrated reporting module within the console to generate reports in multiple formats (pdf, csv, rtf etc.) for performance of	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- MIS- Point no 12 - Reporting & Data Extraction

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				application, network, voice/video applications		
371	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support customization of report with user selectable parameters and graph. It should support per-defined templates for easy customization	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- MIS
372	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should offer capacity management reporting, site-to-site reports, service performance reports etc. It should provide description of metrics used in the reports	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- MIS
373	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support customized scheduling of reports. Solution should have scheduled report be sent in an email as a PDF, RTF, or CSV file attachment	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- System Overview

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
374	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should offer Daily / Weekly / Monthly trend-based reporting	Visibility platform/solution should have this essential feature.	Pls refer Tech Spec of OVP parameter- MIS
375	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must support multiple simultaneous user sessions to the management console. It should support minimum 50 concurrent users and should have facility to create at least 100 Users for sites.	Visibility platform/solution should have this essential feature.	Pls refer revision
376	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide local & remote access on both GUI & CLI based	Visibility platform/solution should have this essential feature.	As per RFP
377	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must provide Role-Based Access Control (RBAC) with TACACS/Radius integration to manage user access rights. i.e., once a user account is	Visibility platform/solution should have this essential feature.	Pls refer Tech spec of OVP- parameter 20- Security and accounting management

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				created, administrators must have the ability to group multiple users with the same privileges and assign access rights to the group or individuals		
378	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The system allows user to create groups based on IP addresses / subnets, interfaces etc. for use in policies, reports, etc.	Visibility platform/solution should have this essential feature.	At GFGNL, our priority is on foundational monitoring features.
379	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution hardware should have redundant, hot-swappable power supplies and Fan Modules	Visibility platform/solution should have this essential feature.	As per RFP
380	59	4.4DDoS - Distributed Denial-of-Service	Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	The performance of a solution is influenced by a combination of hardware and operating system. Specifying generic hardware specifications may limit participation and create an unintended bias	Should support 4x10GbE SFP+ ports, 4x100G QSFP28 ports and must have dual Dual Power supply	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				towards certain manufacturers. As long as the proposed solution is capable of delivering the required performance, the specific hardware and software combination should remain irrelevant. Therefore, we respectfully request the removal of this clause to ensure fair competition and broader participation. Interface requirement are excessive for a service providor off path deployment		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
381	60	4.5Link Load Balancer	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	The performance of a solution is influenced by a combination of hardware and operating system. Specifying generic hardware specifications may limit participation and create an unintended bias towards certain manufacturers. As long as the proposed solution is capable of delivering the required performance, the specific hardware and software combination should remain irrelevant. Therefore, we respectfully request the removal of this clause to ensure fair competition.	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
382	69	4.8 Carrier Grade NAT	The router shall support multicast, routing and protocols	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is relevant only for unicast traffic, and multicast traffic does not traverse this segment of the network. This clause effectively restricts the participation of dedicated CGN solutions in this tender, limiting competition. We therefore request the removal of this clause to ensure a fair and open bidding process.	We request to remove this clause	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
383	-	4.8 Carrier Grade NAT	Should support Multicast protocols like IGMP, PIM, etc	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is relevant only for unicast traffic, and multicast traffic does not traverse this segment of the network. This clause effectively restricts the participation of dedicated CGN solutions in this tender, limiting competition. We therefore request the removal of this clause to ensure a fair and open bidding process.	We request to remove this clause	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
384	70	4.8 Carrier Grade NAT	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
385	70	4.8 Carrier Grade NAT	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	The requirement for passive traffic analysis of mobile devices is essential for maintaining security and visibility within the network. Enhance network monitoring, security, and compliance.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
386	70	4.8 Carrier Grade NAT	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
387	70	4.8 Carrier Grade NAT	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., Net Flow) and the ability to detect deviations from normal baselines.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
388	70	4.8 Carrier Grade NAT	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
389	70	4.8 Carrier Grade NAT	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklistShould must support DNS threat intelligence feeds to protect against threats	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
390	70	4.8 Carrier Grade NAT	Should must support URL threat intelligence feeds to protect against threats	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
391	70	4.8 Carrier Grade NAT	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerence of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The illintend misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due deligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
392	70	4.8 Carrier Grade NAT	Should support safe search for YouTube EDU enforcement	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
393	70	4.8 Carrier Grade NAT	Should support the capability of providing network-based detection of malware by checking the disposition of known/unknown files using SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance (if required in future)	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
394	71	4.8 Carrier Grade NAT	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
395	71	4.8 Carrier Grade NAT	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
396	71	4.8 Carrier Grade NAT	The detection engine should support the capability of detecting variants of known threats, as well as new threats	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
397	71	4.8 Carrier Grade NAT	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
398	71	4.8 Carrier Grade NAT	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
399	69	4.8 Carrier Grade NAT	The appliance-based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one	The specified requirements appear to be derived from a Next-Generation Firewall (NGFW) with Intrusion Prevention System (IPS) functionality. However, Carrier-Grade NAT (CGN) is a purpose-built functionality designed specifically for NAT operations and does not require Deep Packet Inspection (DPI) or IPS capabilities. Including this clause effectively restricts the participation of dedicated CGN solution providers in this RFP, limiting fair competition. We therefore request the removal of this clause to ensure broader participation and a more competitive bidding process.	We request to remove this clause	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
400	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Suggestion:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have built-in bypass as best practice.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
401	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or mitigation capability.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
402	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Suggestion:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
403	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Asked revision can be considered. As per GFGNL requirement, for wider participation LLB and DDoS should be provided on separate devices

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
404	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Asked revision can be considered. As per GFGNL requirement, for wider participation LLB and DDoS should be provided on separate devices

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
405	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	**Hence requesting you to remove this point.**	**Suggestion:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	This clause is relaxed for wider participation

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
406	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Suggestion:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Both Statefull and stateless technology is allowed alongwith corresponding changes to meet functional and performance ask and objectivity.
407	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Suggestion:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
408	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Suggestion:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
409	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Suggestion:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
410	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Suggestion:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
411	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					sophisticated flood attacks.	
412	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
413	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT	**Suggestion:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	
414	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Suggestion:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user productivity and business.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
415	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance	**Suggestion:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				for SSL TPS scalability		
416	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	**Suggestion:** DDoS solution should have capability to detect and mitigate different protocol attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
417	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Suggestion:** For service provider kind of customer, it is recommended to have solution deployed out-of-path for reduced latency.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
418	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Suggestion:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
419	-	4.4 DDoS - Distribute	Additional Clause	Proposed OEM should be deployed and used by at least	Proposed OEM should be deployed and used by at least 2 Tier-1	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		d Denial-of-Service		2 Tier-1 service providers for DDoS mitigation in India	service providers for DDoS mitigation in India	
420	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Suggestion:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
421	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Suggestion:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
422	58	4.4 DDoS - Distributed Denial-of-Service/1	The proposed solution should be a dedicated solution as DDoS protection device, not as add on license Feature on ADC and NGFW.	Proposed appliance must be purpose built system and should be stateless technology not having any kind of state limitation such as TCP connections etc. Proposed appliance should be a dedicated appliance based solution (not a part of Router, UTM, Application Delivery Controller, IPS, Load Balancer,KVM , Proxy based architecture or any Stateful Device)	It is alsways recommended to have dedicated stateless ddos appliance to protect the security stack from state exaustion ddos attacks and shouldn't be part of any statefull devices like ADC,LLB UTM etc.Request you to ammend the clause as suggested for allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices and to avoid any tick mark solution getting quoted which will not help in protecting the organisation from the complex ddos attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
423	59	4.4 DDoS - Distributed Denial-of-Service/2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	System should support 16 x 10G SFP+ ports from day 1 . All the protection ports should support inbuilt Hardware and Software Bypass with Fail-Open and Fail-Closed options. No external bypass switch will be accepted.Dual Power supply. 4 TB or 1 year equalant logs should be kept on device / central management.Same appliance should support 4x100 G fibre bypass interfaces by replacing/upgrading NIC/Interfaces in future.	OEM specific clause and restricting the participation. This is not even practical to keep 4 TB storage on the appliance as every oem has its own different architecture. This specs seems to be supporting some KVM server not the Anti DDOS security appliance.Being fibre grid and the way technology or back plane keeps on changing , 100 G support in future is a must to have .Request you to ammend the clause as suggested for allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
424	59	4.4 DDoS - Distributed Denial-of-Service/3	Device should support at least 80Gbps throughput	System should have a Scalable Clean Throughput License approach for Legitimate Traffic. System should support Clean Throughput License Scalability upto 100 Gbps over next 5 years without changing the appliance.System should support Clean Throughput License of 20 Gbps from day 1 and scalability with a license upgrade.Proposed appliance should support more then 75 Million packet per seconds flood prevention rate on the same appliance. This performance figure must be mentioned in public facing datasheet.Should support latency less than 90 microseconds. Latency should be	The DDOS is sized on the basis of clean traffic throughput & flood prevention rate MPPS count where this provides scalable approach. These are calculated on the basis of the internet bandwidth and scalability.Request you to ammend the clause as suggested for a practical anti DDOS solution and fair participation of DDOS specific OEMs.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				documented in datasheet		
425	59	4.4 DDoS - Distributed Denial-of-Service/7	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack . System must be able to detect and mitigate Spoofed SYN Flood attacks and should support different mechanisms like: a) TCP Authentication b) TCP Out of Sequence Authentication c) HTTP Authentication - Redirect d) HTTP Authentication -	A lot of other functions are missing. Request you to ammend the clause as suggested as these are very common coutnermeasures of anti DDOS for layer 7	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				soft reset e) HTTP Authentication - JavaScript		
426	59	4.4 DDoS - Distributed Denial-of-Service/12	The solution should support Brute Force attack mitigation	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain atleas a million OEMs inhouse (no third party) IOCs to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a	A lot of other functions are missing. Request you to ammend the clause as suggested . Apart from brute force there are many other parameters.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				configurable interval.		
427	59	4.4 DDoS - Distributed Denial-of-Service/13	The solution should support the behaviour based DDOS mitigation.	The solution should support the host behaviour based DDOS mitigation using challenge response or http authentication	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
428	59	4.4 DDoS - Distributed Denial-of-Service/15	The traffic Auto learning threshold can be apply automatically after auto learning completed.	The traffic Auto learning threshold can be apply automatically or manually after auto learning completed.	OEM specific clause and in the production environment it is never recommended to apply auto threshold as that may hamper the production traffic with a single false positive. It has to be vet by the admin and then should be configured accordingly. Request you to ammend the clause as suggested for a fair competitivon and participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
429	59	4.4 DDoS - Distributed Denial-of-Service/17	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,OEM similar solution should be deployed and used by at least 4 Gov/PSU/BFSI customer in India to protect their own Core infrastructure from attacks and proposed solution should support native Integration with ISP clean pipe for preventing the volumetric flood. In case of volumetric flood on premise solution should send signal to the ISP Scrubbing centre for automated scrubbing at the ISP level . Auto signalling should be supported with atleast 4 Tier 1 ISPs Clean pipe services in India	Hybrid architecture is the main part while desising anti DDOS stretegy which is missing in the specification also proof of references are missing. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
430	59	4.4 DDoS - Distributed Denial-of-Service/18	The solution should support Access control list based on inbuilt GeoIP with configurable duration.	System should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown attacks without manual intervention. The system should not depend only on signatures for mitigation of DDoS attacks.It should restrict the IP address from specific segment like from TOR network and Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals	OEM specific clause and not a practical scnerio as if we block certain country traffic it should be blocked permanentnly. Also many other critical details are missing. Request you to change the clause as suggested for a fair competition and participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
431	59	4.4 DDoS - Distributed Denial-of-Service/19	The solution should able to import third party IP database through File or URL.	System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should act as gateway being at the extreme parimeter not allowing such malicious vectors to come inside the DC network.	OEM specific language also seems to be way old funciton. Todays scnerio every security device supports STIX TAXII same is used by CERTIN as well to automate the ingestions of IOCs in any device. DDOS protection being at the extreme parimeter should block such IOCs not only IPs at entry point itself.Request you to ammend the clause as suggested for next gen anti DDOS solution which should get integrated with CERTIN or any third party IOC provider.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
432	60	4.4 DDoS - Distributed Denial-of-Service/20	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP	Solutions should support Active - Active (High Availability) and Active - Passive Deployment. Solution should support inbuilt Fail-Open and Fail-Closed options for Hardware and Software Bypass	OEM specific and not a DDOS protection function as this feature contradicts the purpose of Anti DDOS solution. These are statefull devices feature where Anti DDOS is always recommended to be stateless else the device itself will become prone to the	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				feature on all inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment. No external bypass switch will be accepted.	DDOS attacks.Request you to ammend the clause as suggested for our participation.	
433	60	4.4 DDoS - Distributed Denial-of-Service/23	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	To be deleted	OEM specific and not a DDOS protection function as Anti DDOs is a transparent device and there is no routing on it is done. This seems some OEM is proposing LLB as a DDOS protection appliance. Requesst you to delete the clause as not relevent for any DDOS solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
434	60	4.4 DDoS - Distributed Denial-of-Service/27	The solution shall provide the flexibility of performing configuration via GUI and command base remotely.	The system must have a dedicated management port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must	OEM specific language . The recommended architecture is having out of band management interface along with central management and a GUI on local device for configuration and monitoring.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				not be possible on traffic interfaces, management interfaces must not switch traffic. Proposed Appliance should have inbuilt GUI based monitoring, configuration management, diagnostics and reporting along with provision of Centralize management.		
435	60	4.4 DDoS - Distributed Denial-of-Service/30	The solution shall support the provisioning of the reports - Attack reports - top sources, targets, attack type, Attack Severity Distribution, Attack Source Region	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region.The proposed OEM should have visibility of Tier 1 global ISPs Internet traffic to provide researched feeds of latest attack footprints to the appliance.	Missing other function related to the efficiency of research.Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
436	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must be able to generate summary attack report of daily/weekly/monthly	The solution must be able to generate summary attack report of daily/weekly/monthly. The proposed OEM should provide online portal access to get visibility of global attack trends along with yearly/half yearly reports on global attack trends for the team to define their stretegies for future.	Missing other function related to the efficiency of research and reports which helps admin to take decisions on fine tuning the policies. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
437	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must provide packet capture for debugging.	The solution must provide packet capture for debugging.The proposed solution should be certified for common criteria collaborative Protection Profile	Common criteria is a critical certification to identify the hardened OS of the system.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through. The purpose is wider competition and for that general principles have been laid.
438	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must support the generation of pdf reports containing the detailed statistics and graphs	The solution must support the generation of pdf reports containing the detailed statistics and graphs.Bidder must propose different OEM for the	Must to have clause to create multi layer security architecture as it is recommended to have multiple detection mechanism.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				solution then WAF , IPS , SLB to create a multi layer security architecture.		
439	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution must be on-premises and hardened as per GFGNL Information Security policy	Visibility platform/solution should have this essential feature.	Pls refer preceding response
440	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution must have redundancy at all layer in both GFGNL datacenters .	Visibility platform/solution should have this essential feature.	Pls refer preceding response
441	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide health monitoring of virtual node, end point device for synthetic testing between selected site network and datacenters (Central system in DC/DR and agents on remote location)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
442	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	4. Solution must address and cover all aspects (front-end applications to back-end	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		applications) of network service monitoring and able to decodes and drill down to session/transactions level		
443	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. The solution should provide an end-to-end solution that includes Network Packet capture, Network Packet Broker, Network Performance Monitoring, end-user experience, voice, video monitoring and Synthetic monitoring as an Integrated solution.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
444	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide support for passive and active monitoring of network traffic.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
445	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	7. Solution should be able to monitor end-user network traffic via network devices	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		and/or packet data at the datacenter without additional components / agent on the endpoint or server.		
446	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should be capable of performing suggestive analysis - based traffic anomaly to identify unusual or unexpected events and thresholds within the monitored environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
447	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to baseline metrics and KPIs (Key Performance Indicators) in the monitored environment. Alert should be raised automatically to the respective team in case of any deviations to this baseline	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
448	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Should be able to monitor Internet access / activity in detail, even if the user is behind the proxy server	Visibility platform/solution should have this essential feature.	Pls refer preceding response
449	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Solution must support both IPv4 and IPv6 Protocols.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
450	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Solution should be able to monitor itself i.e., Monitor its health and send appropriate alerts to the system. SSD/HDD, Interface alerts etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
451	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	13. Solution must provide ability to backup and restore configuration files.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
452	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	14. Multi factor authentication / authentication with PIM	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
453	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	15. Packets/Logs must be stored in encrypted format & must be tamper proof	Visibility platform/solution should have this essential feature.	Pls refer preceding response
454	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	16. PCI- DSS: CHD / SAD related information must not be stored and displayed on user console /dashboard (as it will monitor unencrypted traffic)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
455	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	17. The network traffic capture include sensitive and confidential data within the application like user specific information (user name/password), confidential financial information, project information etc. The solution must note store such sensitive/confidenti	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				al application content data to avoid any misuse by NOC/SOC engineer working on the solution. However, solution must capture and store relevant information required for troubleshooting e.g. host information, session information, TCP values, errors/exceptions etc.		
456	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	18. Solution should be capable of performing real-time capture with following options for 24x7x365 network monitoring, advances protocol analysis, deep packet inspection:	Visibility platform/solution should have this essential feature.	Pls refer preceding response
457	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	19. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
458	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	20. The monitoring system must not use a "sampling" approach when collecting packets, which means it must collect & analyse all the packets to characterize data.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
459	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	23. Solution must provide packet analysis of both real-time and historic data. This should be capable of monitoring all conversations and able to analyze packet streams as defined below	Visibility platform/solution should have this essential feature.	Pls refer preceding response
460	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	24. Solution must provide intelligent deep packet capture and analysis capabilities for long-term storage and retrieval of network packets and statistics.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
461	139	6.5 Operational Visibility Platform	Missing Critical functionality	25. Solution should be able to monitor various latencies/Response	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		time involved in between client and server while accessing the application. For example - TCP RTT, Application response time, Client connect time and server connect time etc.		
462	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	26. Solution must support addition customized network and applications protocols-based Monitoring on the TCP and IP stacks.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
463	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	27. Solution should be capable of decrypting SSL and TLS traffic with provided certificates and private keys	Visibility platform/solution should have this essential feature.	Pls refer preceding response
464	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	28. Solution should be able to monitor peak active session for any application for any server (Where application is hosted) for any time duration along with the details of %age	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				of successful transaction.		
465	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	29. Solution should be able to monitor errors if there are any and %age of failed transaction for any application for any server (Where application is hosted) for any time duration along with the details of error code messages for the same to get the root cause of that failure.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
466	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	30. Solution must provide deep packet inspection (DPI).	Visibility platform/solution should have this essential feature.	Pls refer preceding response
467	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	31. Solution should provide detailed packet decode and analysis for a wide range of industry standard protocols and applications, providing detailed decoding of web-	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				based applications protocols, and services such those listed below:		
468	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	32. Solution should be able to monitor wide range of well know applications along with the custom and home-grown application using packets and flows.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
469	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	33. Solution should be able to provide **in-depth monitoring of various databases and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
470	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	34. Solution should have in-depth monitoring for **front end application like HTTP, HTTPS and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
471	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	35. Solution should be able to monitor **Card Processing traffic and should have dedicated**	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		**monitor for the same:**		
472	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	36. Solution should have in-depth monitoring for **MQ protocol (For example MSMQ, IBM MQ) and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
473	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	37. Solution should have **DNS monitoring** features **and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
474	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	38. Solution should have **Active Directory, LDAP and Radius Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
475	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	39. Solution should have **DHCP Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
476	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	40. Solution should have **Certificate Monitor and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
477	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	41. Solution should have **Unified communication** environment monitoring **and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
478	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	42. Solution should have **DHCP Monitor**ing and should have dedicated monitor for the same:	Visibility platform/solution should have this essential feature.	Pls refer preceding response
479	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	43. The network packet flow Switch should support Non Blocking Architecture	Visibility platform/solution should have this essential feature.	Pls refer preceding response
480	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	44. Solution must provide central dashboard for network, application analysis. This must provide	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		comprehensive high-level view of entire network thereby giving quick insight to resolve problems through the dashboard provided.		
481	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	45. Solution shall offer enterprise-wide visibility over the status of all the deployed components from a central dashboard. All the required licenses for analyzing the traffic (For ex- Web, DB, App, UC & Citrix) should be active from day one.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
482	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	46. Solution should be Hybrid in nature offering visibility across on-prim, public cloud, and private cloud from single/unified central management console	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
483	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	47. Solution should support traffic capture and analysis on Private Cloud (using virtual probe or third party vTAP), Containers, Dockers & other virtual Infrastructure. Virtual and physical network functions in Private cloud environments as either a software agent within a multi-tenant Virtual Machine (VM) or a stand-alone, purpose-built VM. The solution must offer monitoring in a private cloud deployment using industry standard ecosystems.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
484	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	48. Solution should alert on the abnormal traffic behaviors such as whether there is a change in application traffic (sudden increases or decreases), drops in response time or	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				if it disappears completely etc.		
485	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	49. Solution should be able to map traffic using IP address of individual host on the network, allowing for easy identification of individual host and associated traffic on the network. The solution should further be able to provide network packet flow diagram to illustrate network communication between multiple application tiers	Visibility platform/solution should have this essential feature.	Pls refer preceding response
486	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	50. Solution must provide a central management console with probes / packet capturing devices being distributed across multiple geographical locations or public/private clouds.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
487	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	51. Solution should be a complete for health monitoring and synthetic testing of application and network devices.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
488	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	Pls refer preceding response
489	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should be able to capture and **process 20 Gbps** (24x7x365 Capturing) of packet data in DC at real time with the average packet size of 800 - 1000 Byte	Visibility platform/solution should have this essential feature.	Pls refer preceding response
490	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should highlight network, application, and server hardware end infrastructures (including virtualized environment) and provide RCA (Root Cause Analysis).	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
491	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. This should provide back in time investigation & troubleshooting. The historical anaysis shall provide session analysis, host analysis, TCP analysys etc. for minimum period of last 7 days.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
492	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should have capability to store at least 12 months of high-level performance data, trend, issues, and events	Visibility platform/solution should have this essential feature.	Pls refer preceding response
493	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Network packet Flow switch should have up to 48 line-rate ports (48 x1/10 GbE) and (6 x 40Gb)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
494	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. The Switch should be supplied with x. Nos – 1 GbE Copper SFPs x. Nos – 1 GbE MM Optics SFP x. Nos – 10 GbE MM Optics SPF+ x. Nos - 40 Gb trascivers	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Along with required Patch Cords		
495	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. The SNMP monitoring solution shall be sized for 10K devices/servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
496	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. The synthetic monitoring shall be sized for 100 endpoints with atleast 20 end points testing concurrently.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
497	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Comprehensive Solution that should have capability to capture packets from all zones defined in GFGNL datacenter network and end user system defined in scope of work	Visibility platform/solution should have this essential feature.	Pls refer preceding response
498	139	6.5 Operational Visibility Platform	Missing Critical functionality	2. End to end solution is from the same vendor	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):				
499	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution is stiched with multi-vendor technologies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
500	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The proposed solution shall provide information of all the errors & its classification within the traffic on dashbaord. The dashboard showing error code distribution graph over time with classification of errors and numbers of errors in each category with ability to drill on any category or even single error.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
501	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	5. There would be multiple capture points within the network. The solution may aggregate the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		traffic. However, it shall maintain visibility of individual capture points. For e.g. if the same traffic is captured before and after firewall, the solution shall show status of the traffic at both captures including time stamp to perform a hop by hop analysis or calculate latency/delay added in between.		
502	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Discover who and where traffic is routed in the Environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
503	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Discover delivery errors for the applications for which traffic is being captured.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
504	139	6.5 Operational Visibility Platform	Missing Critical functionality	8. Enable capture and storage of packet header information when	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		only KPI calculations and data are required		
505	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Enable or disable storing unnecessary user data traffic when required (packet truncation)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
506	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Define and limiting packet sizes in the solution	Visibility platform/solution should have this essential feature.	Pls refer preceding response
507	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Capture the entire packet, Slicing the size of packet, Packet Truncation, Exclude specific packets and Capture only headers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
508	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
509	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Correlation of the collated traffic data from different sources including synthetic testing agent	Visibility platform/solution should have this essential feature.	Pls refer preceding response
510	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Confidential information & sensitive data with Application like User name, Password, Card No, PIN etc. must not be stored by the solution	Visibility platform/solution should have this essential feature.	Pls refer preceding response
511	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	Pls refer preceding response
512	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. In event of GFGNL involving third party / OEM vendors for any troubleshooting activity and the need arising to share packet capture with them for the purpose of analysis, the solution shall be able to export such	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				packet capture data which can be analysed using standard packet decode tool. However, without manual intervention, the solution shall ensure that the shared packet data must not include entire application content data as is to avoid confidentiality issue or security breach.		
513	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Packet loss	Visibility platform/solution should have this essential feature.	Pls refer preceding response
514	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Retransmission rate	Visibility platform/solution should have this essential feature.	Pls refer preceding response
515	139	6.5 Operational Visibility Platform	Missing Critical functionality	3. Retransmission delay	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):				
516	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Round trip time	Visibility platform/solution should have this essential feature.	Pls refer preceding response
517	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Throughput	Visibility platform/solution should have this essential feature.	Pls refer preceding response
518	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Traffic volume	Visibility platform/solution should have this essential feature.	Pls refer preceding response
519	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Number of connections	Visibility platform/solution should have this essential feature.	Pls refer preceding response
520	139	6.5 Operational Visibility	Missing Critical functionality	8. Data transfer time	Visibility platform/solution	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Platform (NMS + OSS + BSS):			should have this essential feature.	
521	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Server response time	Visibility platform/solution should have this essential feature.	Pls refer preceding response
522	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Delivery errors	Visibility platform/solution should have this essential feature.	Pls refer preceding response
523	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Web protocols: HTTP, HTTPS	Visibility platform/solution should have this essential feature.	Pls refer preceding response
524	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Core Services: SNMPv1-3, AD, DNS, DHCP, NTP, LDAP, FTP, SFTP, SMB v1/v2, SCP	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
525	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Email and Desktop: Secure POP3, Secure SMTP, IMAP, MS ActiveSync, NNTP_SSL, Notes, PoP3 etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
526	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Voice: SIP, H232, RTSP, RTP, SCCP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
527	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Multimedia application: SIP, SIP Conference, SCCP, RTP, RTCP, MSRP and Video: H.323 etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
528	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Various MQ Protocols (MSMQ, IBM MQ Protocol etc.)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
529	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Remote Desktop: Microsoft Remote Desktop, Citrix ICA, VMWare and Citrix Channel	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
530	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Along with Citrix ICA solution should support Citrix channel monitoring	Visibility platform/solution should have this essential feature.	Pls refer preceding response
531	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Database: Oracle DB, MySQL, Microsoft Access, DB2, DBASE, MSSQL, MSSQLMON, ORACLE_SRV, ORACLESQL, SQL_SRV, SQLNET	Visibility platform/solution should have this essential feature.	Pls refer preceding response
532	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Routing and others: Syslog, OSPF, BGP, IPsec, GRE	Visibility platform/solution should have this essential feature.	Pls refer preceding response
533	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility for latency , requests and failures for DB Connect, DB Query, DB Modification, DB Create/Drop.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
534	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	2. Solution should provide latency variation over time with database	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		application usage. To get the idea of how latency varies if Usage (bps) varies for DB Connect, DB Query, DB Modification, DB Create/Drop.		
535	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
536	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failure %over time with total request, to get an idea on failure trend on database application.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
537	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code graph distribution for defined period for DB Connect, DB Query and DB Modification, to get	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a detailed idea on error message which are getting generated in between specific client-Server communication transaction.		
538	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide error code distribution for certain period for GET, PUT and POST, to get a detailed idea on error message which are getting generated in between specific client-Server communication.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
539	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Should provide visibility for latency, requests and failures for GET, HEAD and PUT/POST	Visibility platform/solution should have this essential feature.	Pls refer preceding response
540	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide latency variation over time with application usage. To get the idea of how latency varies if	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				application usage varies		
541	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any	Visibility platform/solution should have this essential feature.	Pls refer preceding response
542	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide failure %over time with total request, to get an idea on failure trend	Visibility platform/solution should have this essential feature.	Pls refer preceding response
543	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Should provide visibility for Latency, Requests and Failures for MQ Messages for example open/close, put/get and Put 1.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
544	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	b) Solution should provide latency variation over time with application usage. To get the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		idea of how latency varies if application usage vary.		
545	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
546	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Solution should provide failure %over time with total request, to get an idea on failure trend and also should know which message (open/close, put/get and Put 1) is faling and the reson of the failure.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
547	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Solution should provide error code distribution for certain period for open/close, put/get and Put 1, To get a detailed idea on error message	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				which are getting generated in between specific client-Server communication.		
548	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility for A-AAAA, PTR-NAPTR and PUT/POST queries.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
549	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide latency Variation over time with DNS application usage. It will give idea of how latency varies if DNS query varies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
550	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with DNS application latency if any	Visibility platform/solution should have this essential feature.	Pls refer preceding response
551	139	6.5 Operational Visibility Platform	Missing Critical functionality	4. Solution should provide DNS application failures overview for	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		accessing the DNS application health		
552	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for A-AAAA, PTR-NAPTR and SRV, to get a detailed idea on error message which are getting generated in between specific client-Server communication transaction	Visibility platform/solution should have this essential feature.	Pls refer preceding response
553	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Ability to give latency, requests and failures for DISCOVER, REQUEST, RENEW and Other	Visibility platform/solution should have this essential feature.	Pls refer preceding response
554	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for DISCOVER, REQUEST, RENEW etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
555	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
556	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with requests, gives idea on failure trend and which are being failed, for example DISCOVER, REQUEST, RENEW and requests with %Failed	Visibility platform/solution should have this essential feature.	Pls refer preceding response
557	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Error code distribution, gives detailed error message which is getting generated in between specific client-Server communication with error code count with failed transaction	Visibility platform/solution should have this essential feature.	Pls refer preceding response
558	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	a) Ability to give latency, requests and failures for Authentication, Search & Compare, Modify and Others.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
559	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for Authentication, Modify etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
560	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency).	Visibility platform/solution should have this essential feature.	Pls refer preceding response
561	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with total requests, gives idea on failure trend and which are being failed for ex: Authentication, modify etc. and transaction count with %Failed.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
562	139	6.5 Operational Visibility	Missing Critical functionality	e) Error code distribution gives detailed error	Visibility platform/solution	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Platform (NMS + OSS + BSS):		message which is getting generated in between specific client-Server communication with error code count with failed transaction.	should have this essential feature.	
563	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility on the certificates which are installed on the specific servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
564	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. It should also provide visibility whether certificate is self-signed, or third party signed certificate.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
565	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Certificate monitoring should provide server Name along with count of certificate with details of certificate for example if certificate is ok, if there are any warning or in critical stage.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
566	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. It should also provide us expiry days for certificate.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
567	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide functionalities of setting alerts for the certificate expiry days.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
568	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility in unified communication user plane (SIP etc.) protocol as well as data plane (media - RTP, RTCP etc.) protocols	Visibility platform/solution should have this essential feature.	Pls refer preceding response
569	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution Should provide visibility for latency, requests and failures in Registration and Call Setup	Visibility platform/solution should have this essential feature.	Pls refer preceding response
570	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		idea on performance of number of requests affected with application latency.		
571	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failures over time with total calls, to get an idea on failure trend on session related protocols.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
572	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for call registration and Call setup, to get a detailed information on error messages which are getting generated in between specific node and unified communication server.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
573	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide detailed session analysis for user plane protocol to get detailed information (for	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				example - server name, client name, calling party, called party, CODEC, Avg RT (ms), Start Time, Duration with status) for troubleshooting purposes.		
574	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should provide visibility on network problem in Unified Communication (i.e. Audio Video packets) like Packet Loss, Jitter, Round Trip Delay and packets Out of Sequence along with stream counters over time to monitor QoS Mismatch.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
575	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should provide detailed information about source and destination (For example - QoS, Codec, SSRC, Packet loss and Jitter	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
576	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to provide issues in between called party and calling party with the details like Packet loss, Voice Jitter, Voice Pkt Loss and also solution should provide media Streams details like Average active, Completed and deviation from QoS	Visibility platform/solution should have this essential feature.	Pls refer preceding response
577	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Solution should provide call search option based on IP address and Extension to search the specific call to troubleshoot the issues in between called party and calling party.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
578	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution shall be able to instrument packet in private cloud like VMWare, VMWare NSX, HyperV, Open Stack etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
579	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The solution shall also be able to instrument packets in container, docker and Kubernetiv environement.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
580	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution shall also be able to instrument packets in public cloud like AWS, Azure, Oracle, Google, IBM Softlayer etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
581	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The solution shall be able to understand and work in SDN environments like Cisco ACI, VMWARE VxLAN etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
582	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support VDI (Microsoft, VMware, Citrix etc.) to identify and triage network performance issues impacting VDI based services and identify the root cause of problems. Solution should be able to obtain visibility of VDI infra, including	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				remote access, client, virtualization, Web, front-end, application, and associated database.		
583	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The Packet Flow shall support - aggregation (Fully flexible any-to-any port mapping) - replication, - filtering, - load balancing, and - source port tagging	Visibility platform/solution should have this essential feature.	Pls refer preceding response
584	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The network packet Flow switch should be monitored via Syslog/SNMP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
585	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The Packet Flow Switch should have redundant, hot-swappable power supplies and Fan Module.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
586	139	6.5 Operational Visibility Platform	Missing Critical functionality	4. Monitor Traffic Port Tagging Should Provides identification of	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		traffic based on source network/link using VLAN tagging		
587	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Local and Remote Management - graphical interfaces - CLI - Alerts can be received by any Syslog server or SNMP manager	Visibility platform/solution should have this essential feature.	Pls refer preceding response
588	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must include a comprehensive logging capability to log all the system events and the solution must be able to send the system logs to SIEM /syslog servers and also should be able to send SNMP trap to the SNMP trap receiver system.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
589	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support integration with Email to receive the alerts on the email.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
590	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must be able to perform time synchronization with NTP server	Visibility platform/solution should have this essential feature.	Pls refer preceding response
591	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support integration with Auto ticket logging (ServiceNow)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
592	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support integration with SIEM (ARCSIGHT)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
593	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should support integration with TACACS (Cisco ISE) /PIM (ARCON) for device management for MFA	Visibility platform/solution should have this essential feature.	Pls refer preceding response
594	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should be integrated with SOC, NoC IToM environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
595	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should work seamlessly with all industry standards Data center Software defined network e.g., Cisco ACI for data center infra, SD-WAN, SD-LAN and similar technologies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
596	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Features capturing packets from various WAN appliances	Visibility platform/solution should have this essential feature.	Pls refer preceding response
597	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Supports TAP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
598	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The dashboard should be able to provide different widgets for different components as online analysis to automatically identify which widget/component or tier is	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				contributing to slowness of the monitored transaction.		
599	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Dashboard should be able to show captured traffic for monitoring individual traffic type or applications based on Packet Size or Application type.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
600	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The dashboard should show relevant performance or error messages within the captured packets that are associated with problems for root-cause analysis.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
601	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Dashboard should have analytical capabilities for assisting in identifying the root cause through a multitude of dashboards and reports. The solution should also	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				simplify the operations monitoring process significantly by helping define the correct team to address the problem. e.g., network, application, server, middleware or database teams. The objective is to reduce Mean Time to Identify (MTTI) and Mean Time to Resolve (MTTR)		
602	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Dashboard must include an interactive user interface that allows users to view real-time & historical analysis, flows end-to-end that includes hop-by-hop traffic analytics at each capture point in the flow	Visibility platform/solution should have this essential feature.	Pls refer preceding response
603	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	6. Dashboard should be able to provide usage of multiple dimensions such as network, application, voice	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		and video together on dashboard		
604	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Dashboard should provide real-time monitoring of all traffic being sent from and received to Data center. The monitoring should include parameter such as response times, usage pattern etc. for identifying communication issues between user and application servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
605	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Dashboard must provide an analysis of the condition or health of the network. It should be able to measure counts and response times for every network transaction captured in the Data Centers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
606	139	6.5 Operational Visibility Platform	Missing Critical functionality	9. Dashboard shall provide key metrics for health measurement will	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		be like application and link throughput volume, retransmissions, success/fail transactions, and application error codes.		
607	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Metrics must be presented on a summary panel with chart details, allowing the user to quickly gain insight into the behavior of multiple applications across multiple segments	Visibility platform/solution should have this essential feature.	Pls refer preceding response
608	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Dashboard should be able to provide complete visibility of network activities, end user experience, and application traffic and network performance. It must also provide summarized analysis, breaking down application response time into following components: a) Client/Server	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				response b) Network bandwidth c) Network latency d) Network congestion e) Network protocol (e.g., TCP)		
609	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Dashboard should provide information to identify and isolate to determine whether end-user experience of slowness in accessing of the information is due to a network or an application issue. It should be able to calculate response times for all relevant applications and determine the impact on user experience.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
610	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	13. Solution should be able to detect and alert on network congestion incidents with the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		ability to drill into client, server, application, or user levels to identify the root cause of the problem. It should be further able to measure traffic by user or application, identify bandwidth hogs and provide information about sites/URLs which are being consumed. The solution must be able to identify the root cause of the problem by pinpointing on the entity in question.		
611	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	14. Solution must be able to provide network traffic monitoring and forensics. It should be able to furnish summarized Executive Dashboard and detail traffic analysis dashboard which gives customizable views of network traffic, allowing the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				user to spot potential problems quickly with top ten views of network traffic data. It should give the root cause of bandwidth issues with an intuitive point-and-click interface		
612	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	15. Dashboard configuration should not be limited to pre-defined templates and should be dynamic. There should not be any license limitation on creation of the dashboards in the monitoring system	Visibility platform/solution should have this essential feature.	Pls refer preceding response
613	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should offer an integrated reporting module within the console to generate reports in multiple formats (pdf, csv, rtf etc.) for performance of application, network, voice/video applications	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
614	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support customization of report with user selectable parameters and graph. It should support per-defined templates for easy customization	Visibility platform/solution should have this essential feature.	Pls refer preceding response
615	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should offer capacity management reporting, site-to-site reports, service performance reports etc. It should provide description of metrics used in the reports	Visibility platform/solution should have this essential feature.	Pls refer preceding response
616	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support customized scheduling of reports. Solution should have scheduled report be sent in an email as a PDF, RTF, or CSV file attachment	Visibility platform/solution should have this essential feature.	Pls refer preceding response
617	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	5. Solution should offer Daily / Weekly / Monthly trend-based reporting	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
618	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must support multiple simultaneous user sessions to the management console. It should support minimum 50 concurrent users and should have facility to create at least 100 Users for sites.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
619	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide local & remote access on both GUI & CLI based	Visibility platform/solution should have this essential feature.	Pls refer preceding response
620	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must provide Role-Based Access Control (RBAC) with TACACS/Radius integration to manage user access rights. i.e., once a user account is created, administrators must have the ability to	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				group multiple users with the same privileges and assign access rights to the group or individuals		
621	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The system allows user to create groups based on IP addresses / subnets, interfaces etc. for use in policies, reports, etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
622	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution hardware should have redundant, hot-swappable power supplies and Fan Modules	Visibility platform/solution should have this essential feature.	Pls refer preceding response
623	81	4.14 Server Point 10 Interfacer	Serial Port, 2 x USB 3.2 Gen 1Port,	Serial Port, 2x USB Gen2/Gen3 or 2 USB ports needs to be offered.	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	The requirement for Serial Port and 2 x USB 3.2 Gen 1 Ports is intended to ensure compatibility with various peripherals and industry-standard interfaces. However, bidders may propose equivalent or higher USB specifications (e.g., USB Gen 2 or Gen 3) as long as they meet or exceed the required functionality. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
624	-	Management Features - 2	System tagging giving admin flexibility to provide metadata tags to each System to enable users to filter and sort systems based on userassigned attributes,	System Tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes or the management console should be enabled with elastic search capable of accessing all the information in the single pane of glass.	Every OEM has different way to address this management feature. We are meeting the functionality to address customer requirement.	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
625	82	Industry Standard Compliance	ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3, TLS 1.2, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory	ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.7, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3, TLS 1.2, DMTF Systems Management	Few parameteres are OEM speicifc. Request to modify as mentioned to allow wider participation from leading OEMs.	The specified standards and certifications ensure compatibility, security, and energy efficiency in line with global best practices. To allow wider participation, bidders may offer equivalent or higher specifications, subject to technical evaluation and compliance with the NOC RFP requirements.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			v1.0, ASHRAE A3/A4. Or any equivalent.	Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4. Or any equivalent.		
626	83	Implementation Services and On-Site Comprehensive Warranty Support directly from OEM	Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 +3 years 24 x 7 Proactive warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider or any other agency during the entire contract duration of 7 +3 years.	Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 24 x 7 Proactive warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider or any other agency during the entire contract duration of 7 years.	We can only provide maximum of 7 years of support and services for the supplied equipment. Would request you to relax this clause for wider participation.	Pls see revise MAF addressing your concern.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
627	89	CPU	1 x 16-core latest generation Intel/AMD processor, minimum 2.7 GHz with a boost of 4.1 GHz or higher, 60MB or more cache	2 x 16-core latest generation Intel/AMD processor, minimum 2.7 GHz with a boost of 4.1 GHz or higher, 60MB or more cache	2 x 16 Core CPU required for performance, availability and redundancy. It is also advisable for better throughput of Backup jobs and restoration purpose.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution or combined output without additional cost and dilution in functionalities. The acceptance of request can not be limitation for qualification for others.
628	89	Interface	Serial Port, 2 x USB 3.2 Gen 1Port,	Serial Port, 2x USB Gen2/Gen3 or 2 USB ports needs to be offered.	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	Repeated query
629	90	Bus Slots	4 x PCIe 5.0 or higher slots	2x PCIe 5.0 & 1x PCIe Gen 4.0.	Current ask is OEM specific. Request to modify as mentioned to allow wider participation from leading OEMs.	Slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation.
630	90	Power Supply	Support for 2 x 1600W or higher 80PLUS Platinum hot-plug redundant power supply	Support for 2 x 1400W or higher 80PLUS Platinum hot-plug redundant power supply	Would request you to relax this clause for wider participation.	Slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
631	90	Industry Standard Compliance	ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3 TLS 1.2, DMTF Systems Management Architecture for Server, Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4	ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.7, Redfish API, IPMI 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3 TLS 1.2, DMTF Systems Management Architecture for Server, Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A	Few parameteres are OEM speicifc. Request to modify as mentioned to allow wider participation from leading OEMs.	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
632	91	Warranty	10 year (7 by OEM +3 extendable years by Bidder) 24x7 comprehensive warranty from the server OEM from day one.	7 year 24x7 comprehensive warranty from the server OEM from day one.	We can only provide maximum of 7 years of support and services for the supplied equipment. Would request you to relax this clause for wider participation.	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
633	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Automated traffic diversion to bypass degraded links	Request to change the clause to "The NMS solution should support bandwidth monitoring for specific links to identify bottlenecks during peak hours , with alerting capabilities. Additionally, it should provide capacity utilization and trends analysis reports."	This is not industry generic clause. We requesting to make it industry standard for better understanding.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
634	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Real time bandwith optmization across network segments	Request to change the clause to "The NMS should support bandwidth monitoring to identify bottlenecks during peak hours and generate alerts when utilization exceeds predefined thresholds."	We are keen on focusing the fucnationality hence requested for change.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
635	48	Clause No. 4.2/Sub Clause No. 2(Functional Requirements)	Failure impact analysis for planned maintenance and service continuity.	Request to change the clause to "The NMS should support defining dependencies, displaying live congestion, and automatically creating incidents upon threshold breaches."	This is not industry generic clause. We requesting to make it industry standard for better understanding.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
636	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Detecting and mitigatiing network congestion with traffic engineering	Request to change the clause to "The NMS should detect congestion , generate alert incidents, and automatically assign them to the network engineer for resolution."	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
637	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Path computation and optimzation	Request to remove this clause as this is not the NMS feature/function.	As specified the mentioned NMS in RFP, NMS doenst perform path computations.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
638	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements) Requirements)	Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target.	Request to remove this clause as this is not the NMS feature/function	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
639	48	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements) Requirements)	The proposed solution should be able to clearly visualize the Hop- by-Hop visibility of the Underlay Network at a granular level Sub- Second) for Identifying clear problematic sections on the Glass pane view	Request to change the clause to "The NMS should detect congestion , generate alert incidents, and automatically assign them to the network engineer for resolution." Ultimate objective is to achieve functionality	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
640	49	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Security & Service Management including service provisioning, Inventory management, self-service portal and customer management		-	Pls refer preceding response
641	50	Clause No. 4.2/Sub Clause No. 2 (Functional Requirements)	Proposed solution should follow the standard Large IP network industry template from customer order generation to service provisioning. Activation to Billing and accounting to SLA management etc. It should cover each and every steps/stage in between the entire cycle	We are requesting to modify as :The NMS shall have API to integrate with BSS and other systems and should complete the entire cycle.	-	At GFGNL, Concept of OVP is to provide the functionality of NMS, OSS and BSS with asked minimum specifications.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			irrespective of whether it is explicitly mentioned or not. These systems should be the one and only systems to manage the entire business of the GFGNL which ultimately fulfill the desires of self-sustainability and embarking on growth path to become most successful Large IP network in the state of Gujarat.			
642	51	Clause No. 4.2/Sub Clause No. 3 (Helpdesk & Customer Issue Management & Problem Management)	Advance analytics tools for pain value analysis. Risk Assesment and Risk Mitigation planning of TTs	Request to change the clause to "The NMS should Monitors bandwidth usage, congestion points, and resource utilization to predict and prevent potential failures of risk to the network."	-	At GFGNL, Operation and Maintenance of huge network of Active passive equipment with high demand availability require vigilant system for RCA.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
643	51	Clause No. 4.2/Sub Clause No. 3 (Helpdesk & Customer Issue Management & Problem Management)	Failure Mode and Effects Analysis	Request to change the clause to "The NMS should monitor congestion and their dependencies and visualizing it for better network analysis and management."	We are requesting for change as the clarity in the feature could help us achieve the functional requirement	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
644	51	Clause No. 4.2/Sub Clause No. 3 (Helpdesk & Customer Issue Management & Problem Management)	Provide an option to announce workarounds and solutions to stakeholders efficiently.	Request to change the clause to "The NMS should include an integrated knowledge base to enhance troubleshooting and decision-making."	We are requesting for change as the clarity in the feature could help us achieve the functional requirement	At GFGNL, Operation and Maintenance of huge network of Active passive equipment with high demand availability require vigilant system for RCA.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
645	53	Clause No. 4.2/Sub Clause No. 10 (Performance Management)	Dynamic link and tunnel delay information.	Request to change the clause to "The NMS should support latency monitoring, round-trip time measurement, and packet analysis for enhanced network performance of the links and tunnels."	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
646	54	Clause No. 4.2/Sub Clause No. 19 (Unified Console)	Infrastructure metrics and logs must be tightly integrated into a single consolidated console for managing infrastructure and security events.	Request to change the clause to "The solution should support infrastructure monitoring with centralized log analysis for improved visibility and issue resolution."	-	As per RFP
647	27	Clause No. 3.1.1/Sub Clause No. 5 (Eligibility Criteria)	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project	Request you to amend this clause for maximum participation and modify it to 2 clients of similar projoect in large ISP, PSU/Govt and BFSI	-	For wider participation- 2 clients are allowed. Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			please refer the definition mentioned below .	sector. This will bring more technically and competitve OEM to the said bid.		
648	31	Clause No. 3.2.1 /Sub Clause No. 3 (Technical qualificati on criteria)	Demonstration of prototype/readiness to meet technology led Governance in NMS and OSS H) The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 network elements in any Government, PSU, Bank/ pubic listed company or large-scale IP network- 5 Marks	Requesting to amend and change thje clause to demonstrate support fo 15000 network elements in large ISP or Government or bank or PSU for maximum particiaption from MII OeM. We are recommending Make in India OEM and well recognised and estabilised in NMS domain.	We are recommendong Make In India OEM and recognized and estbalished in NMS domain. This will bring technically, qualified OEM to the said bid and invite healthy competition to the said bid.Suggested Make in India OEM having fromidable presence across the sectors, The clause will go against the Make In India OEM who has been established with Govt and Telecom sector for more than 5 years and having support network elements for 15000 network elements.	Pls See revision
649	31	Clause No. 3.2.1 /Sub Clause No. 5 (Technical qualificati on criteria)	The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 Customers in any Government, PSU, Bank/ pubic listed company or	We are requesting to amend the clause for atleast one reference case demonstarting support for 15000 Customer instead of 50000 Customer in	-	Pls See revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			large-scale IP network. Presentation to be done for Education department live connections- 3 Marks	any Govt/PSU/Public listed company or telecom sector. Allowing established and recognised Make In India OEM will bring more competition.This does not restrict any OEM to participate in the said bid if the criteria will be relaxed.		
650	48	Functional requirements: Scalability & Multi-Vendor Support	The system should support the deployment of at least 20 professional engineers from OEM services for a minimum one-year period for customization and integration needs	Does this mean deployment of manpower at GFGNL premises for customization of the product??	-	Pls see revision
651	48	Functional requirements:Network Discovery, Network optimization & Inventory Management	OEM - EMS-based management for optical IP nodes, falling back to SSH where EMS APIs are unavailable	Complete details required as to a) total how many number of EMS are to be integrated? b) how many EMS support API? What all functionality supported by API? c) how many EMS to be integrated using SSH?? d) is it required to	-	Pls refer Table 2 for types of elements and no of elements, further in Tech spec 22 Network visibility- its mentioned to refer the Backhaul upgrade RFP for visibility requirement

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				interact directly with NE in any case?? if so, how many such elements? What type of protocols are available in nodes in such scenarios		
652	49	Functional requirements: Order & Inventory Management:	Alarm Correlation & Root Cause Analysis (RCA), Incident Notification & Handling and Alarm Logging & Compliance	a) How many no. of alarms/second is expected??	-	At GFGNL, Concept of OVP is to provide the functionality of NMS, OSS and BSS with asked minimum specifications.
653	49	Functional requirements: Order & Inventory Management:	Security & Service Management including service provisioning, Inventory management, self-service portal and customer management	a) How many no. of provisioning requests are expected per month? b) How many no. of users to access NMS and the self service portal?? how many concurrent users?? c) number of customers to be handled as part of BSS solution d) online data retention period in NMS and in BSS solutions	-	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
654	23	Table 2: Network Element (Indicative):	Node types	Details of number of nodes for each node_type to be managed are required	-	Pls see previous response
655	94	4.19	End point Protection of VMs	1. Scope of End point protection software installations - No. of VMs on which the software needs to be installed, VM's distinct Operating Systems (OS), Log retention period requirement. 2. Whether any specific requirement regarding hosting of solution - On premise/ Cloud based. Infrastructure requirement for Hosting the solution to be provisioned by Bidder or can be provided by client.	To calculate compute and storage requirements	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.
656	27	3.1.1	Eligibility Criteria - All the OEM Products including software components must have proven deployment and comissioning with five	This is a restrictive clause to indigenous OEM's, kindly relax number of clients to two.	-	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			clients in this RFP in past 7 years.			
657	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Suggestion:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have built-in bypass as best practice.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
658	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or mitigation capability.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
659	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Suggestion:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.
660	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
661	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
662	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	**Hence requesting you to remove this point.**	**Suggestion:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
663	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Suggestion:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
664	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Suggestion:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
665	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Suggestion:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
666	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Suggestion:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
667	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Suggestion:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
668	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					sophisticated flood attacks.	
669	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
670	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT	**Suggestion:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	
671	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Suggestion:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user productivity and business.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
672	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance	**Suggestion:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				for SSL TPS scalability		
673	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	**Suggestion:** DDoS solution should have capability to detect and mitigate different protocol attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
674	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Suggestion:** For service provider kind of customer, it is recommended to have solution deployed out-of-path for reduced latency.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
675	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Suggestion:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
676	-	4.4 DDoS - Distribute	Additional Clause	Proposed OEM should be deployed and used by at least	Proposed OEM should be deployed and used by at least 2 Tier-1	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		d Denial-of-Service		2 Tier-1 service providers for DDoS mitigation in India	service providers for DDoS mitigation in India	
677	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Suggestion:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
678	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Suggestion:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
679	94	Functionality/Point 1	End point protection software shall be single agent software for NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates	**Change clause to below** End point protection software shall be single agent or dual agent from same OEM For NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates.	As there are multiple functionalities asked in the Clause hence relaxing the clause from single agent to dual agent from same OEM as suggested will allow maximum and broader participation	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
680	57	Interface & Performance / Point 1	The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	**Change clause to below** The proposed appliance should have minimum of 8 x 1/10 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level.	Changing the 8x1/10/25 Gigabit SFP+ Ports to 8x1/10 Gigabit SFP+ will relax the clause and will allow broader participitation also as 4 Port 40/100 G gbps ports are asked hence 35 Gigabit will not have any usability in the solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
681	57	Interface & Performance/Point 2	The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	**Change clause to below** The proposed single appliance should deliver 40 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 60Gbps on stacking supporting 72M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 60 Gbps throughput on stacking having <60 microsec latency	As the Next gen firewall throughput asked in Technical specs section is 60 Gbps hence NIPS throughput must be inline and less to it i.e 40 Gbps also modifing the scalable throughput to 60 Gbps and 72 M Concurrent connections/second and maximum stacking TLS/SSL throughput to 60 Gbps will relax the clause and allow broader participitation and removing OEM Specific stacking functionality	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
682	57	Functionality / Point 2	The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in	**Change clause to below** The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs)	As STIX/TAXII are open platform and blocking may require integration with proposed endopoint solution hence intelligence sharing can happen via endpoint and NIPS integration still it will help to achieve the functionality and allowing broader participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			the NIPS.	to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS or using endpoint tool ,Bidder can propose integration platform to achieve this functionality		
683	58	Functionality / Point 9	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality.	**Change clause to below** Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy or have it own learning mechanism to understand network traffic pattern to create a baseling for anamoly an to shield vulnerabilities	As NIPS itself have signatures hence integration with third party vulnerbaility scanner is not always required hence changing this clause as suggested will relax the clause and allow broader participitaion thus removing OEM specific functionality	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
684	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Suggestion:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have built-in bypass as best practice.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
685	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or mitigation capability.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
686	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Suggestion:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.
687	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
688	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
689	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	**Hence requesting you to remove this point.**	**Suggestion:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
690	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Suggestion:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
691	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Suggestion:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
692	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Suggestion:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
693	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Suggestion:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
694	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Suggestion:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
695	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.
696	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
697	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	**Suggestion:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.
698	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Suggestion:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					productivity and business.	
699	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance for SSL TPS scalability	**Suggestion:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
700	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	**Suggestion:** DDoS solution should have capability to detect and mitigate different protocol attacks.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
701	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Suggestion:** For service provider kind of customer, it is recommended to have solution deployed out-	Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					of-path for reduced latency.	
702	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Suggestion:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.
703	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should be deployed and used by at least 2 Tier-1 service providers for DDoS mitigation in India	Proposed OEM should be deployed and used by at least 2 Tier-1 service providers for DDoS mitigation in India	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
704	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Suggestion:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
705	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Suggestion:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
706	-	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on	**The Bidder should submit below document -** a) CA certified and audited Balance Sheet and Profit & Loss statement for the three financial years considered till	The bidder should have average annual turnover of minimum INR 100 Crores from **IT/ITES/ ICT System** Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	Request to you kindly consider. Relaxing the clause will have wider participation in RFP for healthy competition and larger participation.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		31st March 2024.				

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
707	-	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40	Copies of Purchase Order, completion/ Go-live Certificate or partial completion certificate complying to the clause requirement from client to be enclosed along with Technical Bid.	**The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein:** **a) One project with the value of at least 40 crores with 2.5K SNMP device or** **b) Two projects, each with the value of at least 30 crores with 2K SNMP devices or** **c) Three projects, each with the value of at least 20 crores with 1.5K SNMP devices** **Similar Project is defined as: Implementation, Operation &**	Request to you kindly consider. Relaxing the clause will have wider participation in RFP for healthy competition and larger participation.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or		**Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network as a part of the Project.**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.				

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
708	26	3.1 Qualificati on Criteria	a Bidder shall be deemed to have a Conflict of Interest affecting the Bidding Process, if: • A constituent of the GFGNL Phase III (ABD-Amended Bharatnet Program) RFP or • Such Bidder has the same authorized representative for purposes of this Bid as any other Bidder for the same Package or • For the same Package of GFGNL PH-III RFP, such Bidder, or any Associate thereof has participated as a consultant to GFGNL in the preparation of any documents, design or technical specifications of the Package.	Request you to kindly modify the clause allow the bidders to participate in GFGNL NoC	We have the capability and experience of delivering the NoC projects	As per RFP
709	125	6.1 Scope of Work	6.1.8 SLA-Based DCN Link Monitoring The dimensioning and cost of DCN links connecting BharatNet EMS to S-NOCs (central/state) shall be considered. These links shall be SLA-based with penalties and monitored via the S-NOC.	We understand that DCN Link monitoring connectivity from S-NOCs to BharatNet EMS will be at Delhi BBNL C-NOC or/and Bengaluru BBNL (DR) . Kindly confirm .	This will help to create the correct BoQ as per the requriement	DCN Link BW are to be provided by GFGNL, However Configuration for EMS-NMS is to be done by Bidder where SLA monitoring of links also included

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
710	125	6.1 Scope of Work	6.1.8 SLA-Based DCN Link Monitoring The dimensioning and cost of DCN links connecting BharatNet EMS to S-NOCs (central/state) shall be considered. These links shall be SLA-based with penalties and monitored via the S-NOC.	Kindly share the DCN link bandwidth diemensioning between S-NOCs to BharatNet EMS at BBNL Delhi (C-NOC)	This will help to create the correct BoQ as per the requriement	DCN Link BW are to be provided by GFGNL, However Configuration for EMS-NMS is to be done by Bidder where SLA monitoring of links also included
711	125	6.1 Scope of Work	6.1.8 SLA-Based DCN Link Monitoring The dimensioning and cost of DCN links connecting BharatNet EMS to S-NOCs (central/state) shall be considered. These links shall be SLA-based with penalties and monitored via the S-NOC.	Kindly share the DCN link bandwidth diemensioning between S-NOCs to BharatNet EMS at BBNL Bengaluru (DR)	This will help to create the correct BoQ as per the requriement	DCN Link BW are to be provided by GFGNL, However Configuration for EMS-NMS is to be done by Bidder where SLA monitoring of links also included
712	125	6.1 Scope of Work	6.1.11 DC/DR Sites • The proposed solution should be implemented in DC & DR sites. GFGNL will provide the space and power for DC site at Gandhinagar and DR site at Baroda or other city as per feasibility of GFGNL. • Bidder has to arrange the DR site and connectivity with scalability and availability. • Both the sites shall be in high availability mode.	We understand that DC-DR physical fiber connectivity/bandwidth to be provided by GFGNL free of cost as per the bandwidth requirement between DC-DR. Kindly confirm.	This will help to create the correct BoQ as per the requriement	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
713	111	5.27	Indemnification	The indemnity claimed by GFGNL is very broad and hence Bidder suggests the following for mutual acceptance “Each party shall indemnify the other from and against any claims by third parties (including any governmental authority and expenses (excluding legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such party’s negligence or wilful misconduct”. GFGNL post passing of award make this provision negotiable for the selected bidder is another option for mutual closure.	-	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
714	112	5.28	Limitation of Liability	Please include the following provision within the tender "Bidder's aggregate liability arising out of or in connection with the contract, whether based on contract, tort, statutory warranty or otherwise, shall be limited to an aggregate of most recent 12 months of the charges collected by the bidder under the affected order. The Bidder shall not be liable for any special, indirect, incidental or consequential damages of any kind including but not limited to loss of use, data, profit, income, business, anticipated savings, reputation, and more generally, any loss of an economic or financial nature, whether these may be deemed as	-	Revised Clause for ease of doing business and deburden participants: Selected agency's cumulative liability for its obligations under the contract shall not exceed value of the annual contract applicable for the day claim is raised. Selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				consequential or arising directly and naturally from the incident giving rise to the claim".		
715	113	5.32	Patent Rights, Copy Right &IPR	The indemnity claimed is too broad and hence vendor suggest as under: Vendor shall indemnify and hold harmless GFGNL against any third party claim that any of the vendor's deliverables created or material otherwise provided by vendor hereunder infringes a copyright patent of a third party. GFGNL shall promptly notify vendor of any third party claim and vendor shall at its option conduct the	-	We have already specified in the RFP, Your request is also accepted. Mutually it will be prepared with successful bidder for protecting interest of both parties.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				defence in any such third party action arising as described herein at vendor's sole expense and vendor shall cooperate with such defence. Vendor indemnification shall not extend to any such liability which arises as a result (a) use of vendor's deliverables or services in a manner inconsistent with instructions or documentation provided by vendor; (b) combination of vendor's deliverables or services with software or other programs not provided by vendor.		
716	117	5.4	Risk Purchase	The condition that GFGNL reserves the right to remedied the defects at the risk and cost of the defaulting vendor actually puts the vendor in	-	Pls see revision in MAF

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				UNLIMITED/UNCAPPED RISK which is unreasonable, more due to the fact that there are multiple penalties already applicable. Hence, this paragraph may be deleted.		
717	142 and 124	6.6 Manpower requirement on Payroll of SI and 6.1 (x)	S-NOC shall be manned with qualified manpower for S-NOC operations. S-NOC shall be managed 24x7x365 and accordingly manpower to be planned.	During the O&M of 10 Years manpower is asked to support 24x7x365, whereas as per RFP total total manpower count asked is just 14 for 10 years. Also monitoing of the devices is asked but manpower for monitoring role is not asked in RFP. If bidder consider the additional manpower to provide 24x7x365 operations for L1 or L2 engineers (monitoring , network, server/storage etc) in 3 shifts then the total cost will be significantly higher and can create a	-	Pls see revision in Manpower count. Round the clock manpower is not expected. Per shift minimum 1 no. of L1 support manpower is required to meet operational support including coordination with remaining manpower.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				huge cost difference among various bidders causing a possiblity to get outpriced for the bidder who plan the manpower more accurately. So it is requested that authority may revised the count of manpower requirement as per 24x7x365 availability requirements in 3 shifts. So that all bidders can proposed in a similar manner.		
718	159	Overall O&M Penalty per quarter	The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 20% of Total Quarterly Payable.	20% capping is on higher side, please consider the capping to 10% of quarterly O&M payment.	-	As per RFP
719	65	4.6 / Sr no 11	7+3 extendable years 24x7 comprehensive warranty from the OEM from day one.	Request to be modified as warranty from OEM applicable till end of life announcement from the OEM	Most of the IT & firewall systems warranty is asked for 7 + 3 comprehensive warranty from SI/OEM. Shelf life of line items & support to be considered, request to be modified as	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					warranty with OEM applicable till end of life announcement from the OEM	
720	86	4.15 / Sr no 21	Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 years+ 3 year extendable 24 x 7 warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider during the entire warranty duration of 7+3 years extendable.	Request to be modified as warranty from OEM applicable till end of life announcement from the OEM	Most of the IT systems warranty is asked for 7 + 3 comprehensive warranty from SI/OEM. Shelf life of line items & support to be considered, request to be modified as warranty with OEM applicable till end of life announcement from the OEM	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.
721	103	5.7	Bid Security/ Earnest Money Deposit (EMD)	Exemption of EMD	BEL being a Central Defense PSU, it is requested to exempt the EMD submission for the tender. Please Confirm	Pls see revision
722	118, 153	5.41, 7.5	Submission of PBG	T+3 weeks to be considered or T+2 weeks to be considered. To be clarified	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
723	118	5.41 / Table Sr no 4	Delivery of Hardware for IT Infra and Network infra : T + 6 Weeks	Request to be modified as T + 12 Weeks	To mitigate any unforseen delays in supply chain	The time is essence and we are looking for capable OEMs to meet deliveries. It is the responsibility of bidder to do diligence for timely supply and choosing committed OEMs
724	147	6.8	Bidder shall provide a comprehensive on-site OEM warranty of 7 years and 3 years extended warranty from (SI/OEM) from the date of FAT for proposed solution.	Warranty and CAMC clarity to brought out	Warranty and CAMC clarity to brought out	Pls see revised MAF
725	153	7.5 / Sr no 6 point a)	a) Completion of Installation, Integration, testing of complete network and scope of physical infra and all software as per Project requirement. Integration with BharatNet S-NOC (C-S-NOC) at New Delhi & Bengaluru : T + 15 weeks	Request to be modified as T + 18 Weeks	To mitigate any unforseen delays	The time is essence and we are looking for capable OEMs to meet deliveries. It is the responsibility of bidder to do diligence for timely supply and choosing committed OEMs
726	154	7.5 / Sr no 6 point b)	b) Successful completion of FAT, completion of training and Go-live : T + 17 weeks	T + 21 Weeks	To mitigate any unforseen delays	The time is essence and we are looking for capable OEMs to meet deliveries. It is the responsibility of bidder to do diligence for timely supply and choosing committed OEMs
727	154	7.5 / Sr no 8	Stabilization of the deployed Solution, Security certification and Go-Live. : T + 18 weeks	T + 22 Weeks	To mitigate any unforseen delays	The time is essence and we are looking for capable OEMs to meet deliveries. It is the responsibility of bidder to do diligence for timely supply and choosing committed OEMs
728	23	2.1/ Objective of Phase III (Sr.No: VI)	Ensuring operational efficiency: High network availability to be maintained up to 99% by additional OFC to be laid with 24F/48F Armored	Please confirm that UPS has to be supplied as part of scope of work to every GP. If required, please	-	Said Scope of work is for the reference only to set background for this RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			cable, UPS deployment with minimum 6 Hrs. backup at each GP	provide the UPS power rating, total No of UPS.		
729	129	6.2.10:	ICT Security, Policy, VAPT & Risk Mitigation	It is understood that Bidder has to perform the VAPT of Phase III system.Please confirm that frequency of VAPT audit.	-	Pls refer preceding response
730	58	4.4 DDoS - Distributed Denial-of-Service/1	The proposed solution should be a dedicated solution as DDoS protection device, not as add on license Feature on ADC and NGFW.	Proposed appliance must be purpose built system and should be stateless technology not having any kind of state limitation such as TCP connections etc. Proposed appliance should be a dedicated appliance based solution (not a part of Router, UTM, Application Delivery Controller, IPS, Load Balancer,KVM , Proxy based architecture or any Stateful Device)	It is alsways recommended to have dedicated stateless ddos appliance to protect the security stack from state exaustion ddos attacks and shouldn't be part of any statefull devices like ADC,LLB UTM etc.Request you to ammend the clause as suggested for allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices and to avoid any tick mark solution getting quoted which will not	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					help in protecting the organisation from the complex ddos attacks.	
731	59	4.4 DDoS - Distributed Denial-of-Service/2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	System should support 16 x 10G SFP+ ports from day 1 . All the protection ports should support inbuilt Hardware and Software Bypass with Fail-Open and Fail-Closed options. No external bypass switch will be accepted.Dual Power supply. 4 TB or 1 year equalant logs should be kept on device / central management.Same appliance should support 4x100 G fibre bypass	OEM specific clause and restricting the participation. This is not even practical to keep 4 TB storage on the appliance as every oem has its own different architecture. This specs seems to be supporting some KVM server not the Anti DDOS security appliance.Being fibre grid and the way technology or back plane keeps on changing , 100 G support in future is a must to have .Request you to ammend the clause as suggested for	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				interfaces by replacing/upgrading NIC/Interfaces in future.	allowing the industry leaders to participate which will help the organization in implementing a practical solution with industry best practices.	
732	59	4.4 DDoS - Distributed Denial-of-Service/3	Device should support at least 80Gbps throughput	System should have a Scalable Clean Throughput License approach for Legitimate Traffic. System should support Clean Throughput License Scalability upto 100 Gbps over next 5 years without changing the appliance.System should support Clean Throughput License of 20 Gbps from day 1 and scalability with a license upgrade.Proposed	The DDOS is sized on the basis of clean traffic throughput & flood prevention rate MPPS count where this provides scalable approach. These are calculated on the basis of the internet bandwidth and scalability.Request you to ammend the clause as suggested for a practical anti DDOS solution and fair participation of DDOS specific OEMs.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				appliance should support more then 75 Million packet per seconds flood prevention rate on the same appliance. This performance figure must be mentioned in public facing datasheet.Should support latency less than 90 microseconds. Latency should be documented in datasheet		
733	59	4.4 DDoS - Distributed Denial-of-Service/7	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack . System must be able to detect and mitigate Spoofed SYN Flood attacks and should support different mechanisms like: a) TCP Authentication b) TCP Out of	A lot of other functions are missing. Request you to ammend the clause as suggested as these are very common coutnermeasures of anti DDOS for layer 7	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Sequence Authentication c) HTTP Authentication - Redirect d) HTTP Authentication - soft reset e) HTTP Authentication - JavaScript		
734	59	4.4 DDoS - Distributed Denial-of-Service/12	The solution should support Brute Force attack mitigation	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain atleas a million OEMs inhouse (no third party) IOCs to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a	A lot of other functions are missing. Request you to ammend the clause as suggested . Apart from brute force there are many other parameters.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				configurable interval.		
735	59	4.4 DDoS - Distributed Denial-of-Service/13	The solution should support the behaviour based DDOS mitigation.	The solution should support the host behaviour based DDOS mitigation using challenge response or http authentication	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
736	59	4.4 DDoS - Distributed Denial-of-Service/15	The traffic Auto learning threshold can be apply automatically after auto learning completed.	The traffic Auto learning threshold can be apply automatically or manually after auto learning completed.	OEM specific clause and in the production environment it is never recommended to apply auto threshold as that may hamper the production traffic with a single false positive. It has to be vet by the admin and then should be configured accordingly. Request you to ammend the clause as suggested for a fair competitivon and participation	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
737	59	4.4 DDoS - Distributed Denial-of-Service/17	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,OEM similar solution should be deployed and used by at least 4 Gov/PSU/BFSI customer in India to protect their own Core infrastructure from attacks and proposed solution should support native Integration with ISP clean pipe for preventing the volumetric flood. In case of volumetric flood on premise solution should send signal to the ISP Scrubbing centre for automated scrubbing at the ISP level . Auto signalling should be supported with atleast 4 Tier 1 ISPs Clean pipe services in India	Hybrid architecture is the main part while desising anti DDOS stretegy which is missing in the specification also proof of references are missing. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
738	59	4.4 DDoS - Distributed Denial-of-Service/18	The solution should support Access control list based on inbuilt GeoIP with configurable duration.	System should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown attacks without manual intervention. The system should not depend only on signatures for mitigation of DDoS attacks.It should restrict the IP address from specific segment like from TOR network and Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals	OEM specific clause and not a practical scnerio as if we block certain country traffic it should be blocked permanentnly. Also many other critical details are missing. Request you to change the clause as suggested for a fair competition and participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
739	59	4.4 DDoS - Distributed Denial-of-Service/19	The solution should able to import third party IP database through File or URL.	System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should act as gateway being at the extreme parimeter not allowing such malicious vectors to come inside the DC network.	OEM specific language also seems to be way old funciton. Todays scnerio every security device supports STIX TAXII same is used by CERTIN as well to automate the ingestions of IOCs in any device. DDOS protection being at the extreme parimeter should block such IOCs not only IPs at entry point itself.Request you to ammend the clause as suggested for next gen anti DDOS solution which should get integrated with CERTIN or any third party IOC provider.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
740	60	4.4 DDoS - Distributed Denial-of-Service/20	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP	Solutions should support Active - Active (High Availability) and Active - Passive Deployment. Solution should support inbuilt Fail-Open and Fail-Closed options for Hardware and Software Bypass	OEM specific and not a DDOS protection function as this feature contradicts the purpose of Anti DDOS solution. These are statefull devices feature where Anti DDOS is always recommended to be stateless else the device itself will become prone to the	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				feature on all inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment. No external bypass switch will be accepted.	DDOS attacks.Request you to ammend the clause as suggested for our participation.	
741	60	4.4 DDoS - Distributed Denial-of-Service/23	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	To be deleted	OEM specific and not a DDOS protection function as Anti DDOs is a transparent device and there is no routing on it is done. This seems some OEM is proposing LLB as a DDOS protection appliance. Requesst you to delete the clause as not relevent for any DDOS solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
742	60	4.4 DDoS - Distributed Denial-of-Service/27	The solution shall provide the flexibility of performing configuration via GUI and command base remotely.	The system must have a dedicated management port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must	OEM specific language . The recommended architecture is having out of band management interface along with central management and a GUI on local device for configuration and monitoring.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				not be possible on traffic interfaces, management interfaces must not switch traffic. Proposed Appliance should have inbuilt GUI based monitoring, configuration management, diagnostics and reporting along with provision of Centralize management.		
743	60	4.4 DDoS - Distributed Denial-of-Service/30	The solution shall support the provisioning of the reports - Attack reports - top sources, targets, attack type, Attack Severity Distribution, Attack Source Region	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region.The proposed OEM should have visibility of Tier 1 global ISPs Internet traffic to provide researched feeds of latest attack footprints to the appliance.	Missing other function related to the efficiency of research.Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
744	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must be able to generate summary attack report of daily/weekly/monthly	The solution must be able to generate summary attack report of daily/weekly/monthly. The proposed OEM should provide online portal access to get visibility of global attack trends along with yearly/half yearly reports on global attack trends for the team to define their stretegies for future.	Missing other function related to the efficiency of research and reports which helps admin to take decisions on fine tuning the policies. Request you to ammend the clause as suggested.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
745	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must provide packet capture for debugging.	The solution must provide packet capture for debugging.The proposed solution should be certified for common criteria collaborative Protection Profile	Common criteria is a critical certification to identify the hardened OS of the system.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
746	60	4.4 DDoS - Distributed Denial-of-Service/31	The solution must support the generation of pdf reports containing the detailed statistics and graphs	The solution must support the generation of pdf reports containing the detailed statistics and graphs.Bidder must propose different OEM for the	Must to have clause to create multi layer security architecture as it is recommended to have multiple detection mechanism.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				solution then WAF , IPS , SLB to create a multi layer security architecture.		
747	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution must be on-premises and hardened as per GFGNL Information Security policy	Visibility platform/solution should have this essential feature.	Pls refer preceding response
748	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution must have redundancy at all layer in both GFGNL datacenters .	Visibility platform/solution should have this essential feature.	Pls refer preceding response
749	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide health monitoring of virtual node, end point device for synthetic testing between selected site network and datacenters (Central system in DC/DR and agents on remote location)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
750	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	4. Solution must address and cover all aspects (front-end applications to back-end	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		applications) of network service monitoring and able to decodes and drill down to session/transactions level		
751	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. The solution should provide an end-to-end solution that includes Network Packet capture, Network Packet Broker, Network Performance Monitoring, end-user experience, voice, video monitoring and Synthetic monitoring as an Integrated solution.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
752	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide support for passive and active monitoring of network traffic.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
753	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	7. Solution should be able to monitor end-user network traffic via network devices	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		and/or packet data at the datacenter without additional components / agent on the endpoint or server.		
754	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should be capable of performing suggestive analysis - based traffic anomaly to identify unusual or unexpected events and thresholds within the monitored environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
755	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to baseline metrics and KPIs (Key Performance Indicators) in the monitored environment. Alert should be raised automatically to the respective team in case of any deviations to this baseline	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
756	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Should be able to monitor Internet access / activity in detail, even if the user is behind the proxy server	Visibility platform/solution should have this essential feature.	Pls refer preceding response
757	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Solution must support both IPv4 and IPv6 Protocols.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
758	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Solution should be able to monitor itself i.e., Monitor its health and send appropriate alerts to the system. SSD/HDD, Interface alerts etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
759	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	13. Solution must provide ability to backup and restore configuration files.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
760	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	14. Multi factor authentication / authentication with PIM	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
761	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	15. Packets/Logs must be stored in encrypted format & must be tamper proof	Visibility platform/solution should have this essential feature.	Pls refer preceding response
762	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	16. PCI- DSS: CHD / SAD related information must not be stored and displayed on user console /dashboard (as it will monitor unencrypted traffic)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
763	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	17. The network traffic capture include sensitive and confidential data within the application like user specific information (user name/password), confidential financial information, project information etc. The solution must note store such sensitive/confidenti	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				al application content data to avoid any misuse by NOC/SOC engineer working on the solution. However, solution must capture and store relevant information required for troubleshooting e.g. host information, session information, TCP values, errors/exceptions etc.		
764	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	18. Solution should be capable of performing real-time capture with following options for 24x7x365 network monitoring, advances protocol analysis, deep packet inspection:	Visibility platform/solution should have this essential feature.	Pls refer preceding response
765	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	19. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
766	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	20. The monitoring system must not use a "sampling" approach when collecting packets, which means it must collect & analyse all the packets to characterize data.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
767	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	23. Solution must provide packet analysis of both real-time and historic data. This should be capable of monitoring all conversations and able to analyze packet streams as defined below	Visibility platform/solution should have this essential feature.	Pls refer preceding response
768	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	24. Solution must provide intelligent deep packet capture and analysis capabilities for long-term storage and retrieval of network packets and statistics.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
769	139	6.5 Operational Visibility Platform	Missing Critical functionality	25. Solution should be able to monitor various latencies/Response	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		time involved in between client and server while accessing the application. For example - TCP RTT, Application response time, Client connect time and server connect time etc.		
770	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	26. Solution must support addition customized network and applications protocols-based Monitoring on the TCP and IP stacks.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
771	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	27. Solution should be capable of decrypting SSL and TLS traffic with provided certificates and private keys	Visibility platform/solution should have this essential feature.	Pls refer preceding response
772	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	28. Solution should be able to monitor peak active session for any application for any server (Where application is hosted) for any time duration along with the details of %age	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				of successful transaction.		
773	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	29. Solution should be able to monitor errors if there are any and %age of failed transaction for any application for any server (Where application is hosted) for any time duration along with the details of error code messages for the same to get the root cause of that failure.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
774	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	30. Solution must provide deep packet inspection (DPI).	Visibility platform/solution should have this essential feature.	Pls refer preceding response
775	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	31. Solution should provide detailed packet decode and analysis for a wide range of industry standard protocols and applications, providing detailed decoding of web-	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				based applications protocols, and services such those listed below:		
776	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	32. Solution should be able to monitor wide range of well know applications along with the custom and home-grown application using packets and flows.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
777	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	33. Solution should be able to provide **in-depth monitoring of various databases and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
778	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	34. Solution should have in-depth monitoring for **front end application like HTTP, HTTPS and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
779	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	35. Solution should be able to monitor **Card Processing traffic and should have dedicated**	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		**monitor for the same:**		
780	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	36. Solution should have in-depth monitoring for **MQ protocol (For example MSMQ, IBM MQ) and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
781	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	37. Solution should have **DNS monitoring** features **and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
782	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	38. Solution should have **Active Directory, LDAP and Radius Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
783	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	39. Solution should have **DHCP Monitoring and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
784	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	40. Solution should have **Certificate Monitor and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
785	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	41. Solution should have **Unified communication** environment monitoring **and should have dedicated monitor for the same:**	Visibility platform/solution should have this essential feature.	Pls refer preceding response
786	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	42. Solution should have **DHCP Monitor**ing and should have dedicated monitor for the same:	Visibility platform/solution should have this essential feature.	Pls refer preceding response
787	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	43. The network packet flow Switch should support Non Blocking Architecture	Visibility platform/solution should have this essential feature.	Pls refer preceding response
788	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	44. Solution must provide central dashboard for network, application analysis. This must provide	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		comprehensive high-level view of entire network thereby giving quick insight to resolve problems through the dashboard provided.		
789	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	45. Solution shall offer enterprise-wide visibility over the status of all the deployed components from a central dashboard. All the required licenses for analyzing the traffic (For ex- Web, DB, App, UC & Citrix) should be active from day one.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
790	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	46. Solution should be Hybrid in nature offering visibility across on-prim, public cloud, and private cloud from single/unified central management console	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
791	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	47. Solution should support traffic capture and analysis on Private Cloud (using virtual probe or third party vTAP), Containers, Dockers & other virtual Infrastructure. Virtual and physical network functions in Private cloud environments as either a software agent within a multi-tenant Virtual Machine (VM) or a stand-alone, purpose-built VM. The solution must offer monitoring in a private cloud deployment using industry standard ecosystems.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
792	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	48. Solution should alert on the abnormal traffic behaviors such as whether there is a change in application traffic (sudden increases or decreases), drops in response time or	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				if it disappears completely etc.		
793	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	49. Solution should be able to map traffic using IP address of individual host on the network, allowing for easy identification of individual host and associated traffic on the network. The solution should further be able to provide network packet flow diagram to illustrate network communication between multiple application tiers	Visibility platform/solution should have this essential feature.	Pls refer preceding response
794	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	50. Solution must provide a central management console with probes / packet capturing devices being distributed across multiple geographical locations or public/private clouds.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
795	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	51. Solution should be a complete for health monitoring and synthetic testing of application and network devices.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
796	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. All required licenses to enable all the features shall be provided in each probe from day one	Visibility platform/solution should have this essential feature.	Pls refer preceding response
797	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should be able to capture and **process 20 Gbps** (24x7x365 Capturing) of packet data in DC at real time with the average packet size of 800 - 1000 Byte	Visibility platform/solution should have this essential feature.	Pls refer preceding response
798	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should highlight network, application, and server hardware end infrastructures (including virtualized environment) and provide RCA (Root Cause Analysis).	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
799	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. This should provide back in time investigation & troubleshooting. The historical anaysis shall provide session analysis, host analysis, TCP analysys etc. for minimum period of last 7 days.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
800	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should have capability to store at least 12 months of high-level performance data, trend, issues, and events	Visibility platform/solution should have this essential feature.	Pls refer preceding response
801	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Network packet Flow switch should have up to 48 line-rate ports (48 x1/10 GbE) and (6 x 40Gb)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
802	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. The Switch should be supplied with x. Nos – 1 GbE Copper SFPs x. Nos – 1 GbE MM Optics SFP x. Nos – 10 GbE MM Optics SPF+ x. Nos - 40 Gb trascivers	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Along with required Patch Cords		
803	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. The SNMP monitoring solution shall be sized for 10K devices/servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
804	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. The synthetic monitoring shall be sized for 100 endpoints with atleast 20 end points testing concurrently.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
805	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Comprehensive Solution that should have capability to capture packets from all zones defined in GFGNL datacenter network and end user system defined in scope of work	Visibility platform/solution should have this essential feature.	Pls refer preceding response
806	139	6.5 Operational Visibility Platform	Missing Critical functionality	2. End to end solution is from the same vendor	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):				
807	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution is stiched with multi-vendor technologies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
808	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The proposed solution shall provide information of all the errors & its classification within the traffic on dashbaord. The dashboard showing error code distribution graph over time with classification of errors and numbers of errors in each category with ability to drill on any category or even single error.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
809	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	5. There would be multiple capture points within the network. The solution may aggregate the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		traffic. However, it shall maintain visibility of individual capture points. For e.g. if the same traffic is captured before and after firewall, the solution shall show status of the traffic at both captures including time stamp to perform a hop by hop analysis or calculate latency/delay added in between.		
810	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Discover who and where traffic is routed in the Environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
811	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Discover delivery errors for the applications for which traffic is being captured.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
812	139	6.5 Operational Visibility Platform	Missing Critical functionality	8. Enable capture and storage of packet header information when	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		only KPI calculations and data are required		
813	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Enable or disable storing unnecessary user data traffic when required (packet truncation)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
814	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Define and limiting packet sizes in the solution	Visibility platform/solution should have this essential feature.	Pls refer preceding response
815	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Capture the entire packet, Slicing the size of packet, Packet Truncation, Exclude specific packets and Capture only headers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
816	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
817	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Correlation of the collated traffic data from different sources including synthetic testing agent	Visibility platform/solution should have this essential feature.	Pls refer preceding response
818	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Confidential information & sensitive data with Application like User name, Password, Card No, PIN etc. must not be stored by the solution	Visibility platform/solution should have this essential feature.	Pls refer preceding response
819	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. User Defined criteria customised capture	Visibility platform/solution should have this essential feature.	Pls refer preceding response
820	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. In event of GFGNL involving third party / OEM vendors for any troubleshooting activity and the need arising to share packet capture with them for the purpose of analysis, the solution shall be able to export such	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				packet capture data which can be analysed using standard packet decode tool. However, without manual intervention, the solution shall ensure that the shared packet data must not include entire application content data as is to avoid confidentiality issue or security breach.		
821	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Packet loss	Visibility platform/solution should have this essential feature.	Pls refer preceding response
822	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Retransmission rate	Visibility platform/solution should have this essential feature.	Pls refer preceding response
823	139	6.5 Operational Visibility Platform	Missing Critical functionality	3. Retransmission delay	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):				
824	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Round trip time	Visibility platform/solution should have this essential feature.	Pls refer preceding response
825	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Throughput	Visibility platform/solution should have this essential feature.	Pls refer preceding response
826	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Traffic volume	Visibility platform/solution should have this essential feature.	Pls refer preceding response
827	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Number of connections	Visibility platform/solution should have this essential feature.	Pls refer preceding response
828	139	6.5 Operational Visibility	Missing Critical functionality	8. Data transfer time	Visibility platform/solution	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Platform (NMS + OSS + BSS):			should have this essential feature.	
829	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Server response time	Visibility platform/solution should have this essential feature.	Pls refer preceding response
830	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Delivery errors	Visibility platform/solution should have this essential feature.	Pls refer preceding response
831	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Web protocols: HTTP, HTTPS	Visibility platform/solution should have this essential feature.	Pls refer preceding response
832	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Core Services: SNMPv1-3, AD, DNS, DHCP, NTP, LDAP, FTP, SFTP, SMB v1/v2, SCP	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
833	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Email and Desktop: Secure POP3, Secure SMTP, IMAP, MS ActiveSync, NNTP_SSL, Notes, PoP3 etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
834	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Voice: SIP, H232, RTSP, RTP, SCCP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
835	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Multimedia application: SIP, SIP Conference, SCCP, RTP, RTCP, MSRP and Video: H.323 etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
836	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Various MQ Protocols (MSMQ, IBM MQ Protocol etc.)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
837	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Remote Desktop: Microsoft Remote Desktop, Citrix ICA, VMWare and Citrix Channel	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
838	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Along with Citrix ICA solution should support Citrix channel monitoring	Visibility platform/solution should have this essential feature.	Pls refer preceding response
839	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Database: Oracle DB, MySQL, Microsoft Access, DB2, DBASE, MSSQL, MSSQLMON, ORACLE_SRV, ORACLESQL, SQL_SRV, SQLNET	Visibility platform/solution should have this essential feature.	Pls refer preceding response
840	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Routing and others: Syslog, OSPF, BGP, IPsec, GRE	Visibility platform/solution should have this essential feature.	Pls refer preceding response
841	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility for latency , requests and failures for DB Connect, DB Query, DB Modification, DB Create/Drop.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
842	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	2. Solution should provide latency variation over time with database	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		application usage. To get the idea of how latency varies if Usage (bps) varies for DB Connect, DB Query, DB Modification, DB Create/Drop.		
843	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
844	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failure %over time with total request, to get an idea on failure trend on database application.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
845	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code graph distribution for defined period for DB Connect, DB Query and DB Modification, to get	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a detailed idea on error message which are getting generated in between specific client-Server communication transaction.		
846	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide error code distribution for certain period for GET, PUT and POST, to get a detailed idea on error message which are getting generated in between specific client-Server communication.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
847	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Should provide visibility for latency, requests and failures for GET, HEAD and PUT/POST	Visibility platform/solution should have this essential feature.	Pls refer preceding response
848	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide latency variation over time with application usage. To get the idea of how latency varies if	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				application usage varies		
849	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any	Visibility platform/solution should have this essential feature.	Pls refer preceding response
850	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide failure %over time with total request, to get an idea on failure trend	Visibility platform/solution should have this essential feature.	Pls refer preceding response
851	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Should provide visibility for Latency, Requests and Failures for MQ Messages for example open/close, put/get and Put 1.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
852	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	b) Solution should provide latency variation over time with application usage. To get the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		idea of how latency varies if application usage vary.		
853	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with application latency if any.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
854	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Solution should provide failure %over time with total request, to get an idea on failure trend and also should know which message (open/close, put/get and Put 1) is faling and the reson of the failure.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
855	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Solution should provide error code distribution for certain period for open/close, put/get and Put 1, To get a detailed idea on error message	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				which are getting generated in between specific client-Server communication.		
856	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility for A-AAAA, PTR-NAPTR and PUT/POST queries.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
857	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide latency Variation over time with DNS application usage. It will give idea of how latency varies if DNS query varies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
858	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an idea on numbers of request, FAST, Degraded, Slow and timeouts with DNS application latency if any	Visibility platform/solution should have this essential feature.	Pls refer preceding response
859	139	6.5 Operational Visibility Platform	Missing Critical functionality	4. Solution should provide DNS application failures overview for	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		accessing the DNS application health		
860	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for A-AAAA, PTR-NAPTR and SRV, to get a detailed idea on error message which are getting generated in between specific client-Server communication transaction	Visibility platform/solution should have this essential feature.	Pls refer preceding response
861	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	a) Ability to give latency, requests and failures for Authentication, Search & Compare, Modify and Others.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
862	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for Authentication, Modify etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
863	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency).	Visibility platform/solution should have this essential feature.	Pls refer preceding response
864	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with total requests, gives idea on failure trend and which are being failed for ex: Authentication, modify etc. and transaction count with %Failed.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
865	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	e) Error code distribution gives detailed error message which is getting generated in between specific client-Server communication with error code count with failed transaction.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
866	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	a) Ability to give latency, requests and failures for DISCOVER,	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		REQUEST, RENEW and Other		
867	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	b) Latency Variation over time with application usage. It will give idea of how latency varies based on usage for DISCOVER, REQUEST, RENEW etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
868	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	c) Performance variation over Latency. (Gives idea on numbers of request, FAST, Degraded, Slow and timeouts with transaction count and latency)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
869	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	d) Failure %over time with requests, gives idea on failure trend and which are being failed, for example DISCOVER, REQUEST, RENEW and requests with %Failed	Visibility platform/solution should have this essential feature.	Pls refer preceding response
870	139	6.5 Operational Visibility Platform	Missing Critical functionality	e) Error code distribution, gives detailed error message which is	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		getting generated in between specific client-Server communication with error code count with failed transaction		
871	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Should provide visibility on the certificates which are installed on the specific servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
872	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. It should also provide visibility whether certificate is self-signed, or third party signed certificate.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
873	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Certificate monitoring should provide server Name along with count of certificate with details of certificate for example if certificate is ok, if there are any warning or in critical stage.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
874	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. It should also provide us expiry days for certificate.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
875	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide functionalities of setting alerts for the certificate expiry days.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
876	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should provide visibility in unified communication user plane (SIP etc.) protocol as well as data plane (media - RTP, RTCP etc.) protocols	Visibility platform/solution should have this essential feature.	Pls refer preceding response
877	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution Should provide visibility for latency, requests and failures in Registration and Call Setup	Visibility platform/solution should have this essential feature.	Pls refer preceding response
878	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	3. Solution should provide performance variation over Latency. To get an	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		idea on performance of number of requests affected with application latency.		
879	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should provide failures over time with total calls, to get an idea on failure trend on session related protocols.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
880	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should provide error code distribution for defined period for call registration and Call setup, to get a detailed information on error messages which are getting generated in between specific node and unified communication server.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
881	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should provide detailed session analysis for user plane protocol to get detailed information (for	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				example - server name, client name, calling party, called party, CODEC, Avg RT (ms), Start Time, Duration with status) for troubleshooting purposes.		
882	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should provide visibility on network problem in Unified Communication (i.e. Audio Video packets) like Packet Loss, Jitter, Round Trip Delay and packets Out of Sequence along with stream counters over time to monitor QoS Mismatch.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
883	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should provide detailed information about source and destination (For example - QoS, Codec, SSRC, Packet loss and Jitter	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
884	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Solution should be able to provide issues in between called party and calling party with the details like Packet loss, Voice Jitter, Voice Pkt Loss and also solution should provide media Streams details like Average active, Completed and deviation from QoS	Visibility platform/solution should have this essential feature.	Pls refer preceding response
885	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Solution should provide call search option based on IP address and Extension to search the specific call to troubleshoot the issues in between called party and calling party.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
886	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The solution shall be able to instrument packet in private cloud like VMWare, VMWare NSX, HyperV, Open Stack etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
887	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The solution shall also be able to instrument packets in container, docker and Kubernetiv environement.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
888	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The solution shall also be able to instrument packets in public cloud like AWS, Azure, Oracle, Google, IBM Softlayer etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
889	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The solution shall be able to understand and work in SDN environments like Cisco ACI, VMWARE VxLAN etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
890	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support VDI (Microsoft, VMware, Citrix etc.) to identify and triage network performance issues impacting VDI based services and identify the root cause of problems. Solution should be able to obtain visibility of VDI infra, including	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				remote access, client, virtualization, Web, front-end, application, and associated database.		
891	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The Packet Flow shall support - aggregation (Fully flexible any-to-any port mapping) - replication, - filtering, - load balancing, and - source port tagging	Visibility platform/solution should have this essential feature.	Pls refer preceding response
892	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. The network packet Flow switch should be monitored via Syslog/SNMP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
893	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The Packet Flow Switch should have redundant, hot-swappable power supplies and Fan Module.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
894	139	6.5 Operational Visibility Platform	Missing Critical functionality	4. Monitor Traffic Port Tagging Should Provides identification of	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		traffic based on source network/link using VLAN tagging		
895	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Local and Remote Management - graphical interfaces - CLI - Alerts can be received by any Syslog server or SNMP manager	Visibility platform/solution should have this essential feature.	Pls refer preceding response
896	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must include a comprehensive logging capability to log all the system events and the solution must be able to send the system logs to SIEM /syslog servers and also should be able to send SNMP trap to the SNMP trap receiver system.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
897	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support integration with Email to receive the alerts on the email.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
898	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must be able to perform time synchronization with NTP server	Visibility platform/solution should have this essential feature.	Pls refer preceding response
899	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support integration with Auto ticket logging (ServiceNow)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
900	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution should support integration with SIEM (ARCSIGHT)	Visibility platform/solution should have this essential feature.	Pls refer preceding response
901	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	6. Solution should support integration with TACACS (Cisco ISE) /PIM (ARCON) for device management for MFA	Visibility platform/solution should have this essential feature.	Pls refer preceding response
902	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Solution should be integrated with SOC, NoC IToM environment.	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
903	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Solution should work seamlessly with all industry standards Data center Software defined network e.g., Cisco ACI for data center infra, SD-WAN, SD-LAN and similar technologies	Visibility platform/solution should have this essential feature.	Pls refer preceding response
904	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	9. Features capturing packets from various WAN appliances	Visibility platform/solution should have this essential feature.	Pls refer preceding response
905	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Supports TAP	Visibility platform/solution should have this essential feature.	Pls refer preceding response
906	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. The dashboard should be able to provide different widgets for different components as online analysis to automatically identify which widget/component or tier is	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				contributing to slowness of the monitored transaction.		
907	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Dashboard should be able to show captured traffic for monitoring individual traffic type or applications based on Packet Size or Application type.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
908	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. The dashboard should show relevant performance or error messages within the captured packets that are associated with problems for root-cause analysis.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
909	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Dashboard should have analytical capabilities for assisting in identifying the root cause through a multitude of dashboards and reports. The solution should also	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				simplify the operations monitoring process significantly by helping define the correct team to address the problem. e.g., network, application, server, middleware or database teams. The objective is to reduce Mean Time to Identify (MTTI) and Mean Time to Resolve (MTTR)		
910	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Dashboard must include an interactive user interface that allows users to view real-time & historical analysis, flows end-to-end that includes hop-by-hop traffic analytics at each capture point in the flow	Visibility platform/solution should have this essential feature.	Pls refer preceding response
911	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	6. Dashboard should be able to provide usage of multiple dimensions such as network, application, voice	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		and video together on dashboard		
912	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	7. Dashboard should provide real-time monitoring of all traffic being sent from and received to Data center. The monitoring should include parameter such as response times, usage pattern etc. for identifying communication issues between user and application servers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
913	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	8. Dashboard must provide an analysis of the condition or health of the network. It should be able to measure counts and response times for every network transaction captured in the Data Centers.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
914	139	6.5 Operational Visibility Platform	Missing Critical functionality	9. Dashboard shall provide key metrics for health measurement will	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(NMS + OSS + BSS):		be like application and link throughput volume, retransmissions, success/fail transactions, and application error codes.		
915	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	10. Metrics must be presented on a summary panel with chart details, allowing the user to quickly gain insight into the behavior of multiple applications across multiple segments	Visibility platform/solution should have this essential feature.	Pls refer preceding response
916	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	11. Dashboard should be able to provide complete visibility of network activities, end user experience, and application traffic and network performance. It must also provide summarized analysis, breaking down application response time into following components: a) Client/Server	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				response b) Network bandwidth c) Network latency d) Network congestion e) Network protocol (e.g., TCP)		
917	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	12. Dashboard should provide information to identify and isolate to determine whether end-user experience of slowness in accessing of the information is due to a network or an application issue. It should be able to calculate response times for all relevant applications and determine the impact on user experience.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
918	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	13. Solution should be able to detect and alert on network congestion incidents with the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):		ability to drill into client, server, application, or user levels to identify the root cause of the problem. It should be further able to measure traffic by user or application, identify bandwidth hogs and provide information about sites/URLs which are being consumed. The solution must be able to identify the root cause of the problem by pinpointing on the entity in question.		
919	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	14. Solution must be able to provide network traffic monitoring and forensics. It should be able to furnish summarized Executive Dashboard and detail traffic analysis dashboard which gives customizable views of network traffic, allowing the	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				user to spot potential problems quickly with top ten views of network traffic data. It should give the root cause of bandwidth issues with an intuitive point-and-click interface		
920	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	15. Dashboard configuration should not be limited to pre-defined templates and should be dynamic. There should not be any license limitation on creation of the dashboards in the monitoring system	Visibility platform/solution should have this essential feature.	Pls refer preceding response
921	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution should offer an integrated reporting module within the console to generate reports in multiple formats (pdf, csv, rtf etc.) for performance of application, network, voice/video applications	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
922	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should support customization of report with user selectable parameters and graph. It should support per-defined templates for easy customization	Visibility platform/solution should have this essential feature.	Pls refer preceding response
923	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution should offer capacity management reporting, site-to-site reports, service performance reports etc. It should provide description of metrics used in the reports	Visibility platform/solution should have this essential feature.	Pls refer preceding response
924	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. Solution should support customized scheduling of reports. Solution should have scheduled report be sent in an email as a PDF, RTF, or CSV file attachment	Visibility platform/solution should have this essential feature.	Pls refer preceding response
925	139	6.5 Operational Visibility Platform (NMS +	Missing Critical functionality	5. Solution should offer Daily / Weekly / Monthly trend-based reporting	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		OSS + BSS):				
926	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	1. Solution must support multiple simultaneous user sessions to the management console. It should support minimum 50 concurrent users and should have facility to create at least 100 Users for sites.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
927	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	2. Solution should provide local & remote access on both GUI & CLI based	Visibility platform/solution should have this essential feature.	Pls refer preceding response
928	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	3. Solution must provide Role-Based Access Control (RBAC) with TACACS/Radius integration to manage user access rights. i.e., once a user account is created, administrators must have the ability to	Visibility platform/solution should have this essential feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				group multiple users with the same privileges and assign access rights to the group or individuals		
929	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	4. The system allows user to create groups based on IP addresses / subnets, interfaces etc. for use in policies, reports, etc.	Visibility platform/solution should have this essential feature.	Pls refer preceding response
930	139	6.5 Operational Visibility Platform (NMS + OSS + BSS):	Missing Critical functionality	5. Solution hardware should have redundant, hot-swappable power supplies and Fan Modules	Visibility platform/solution should have this essential feature.	Pls refer preceding response
931	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional**	Automated traffic diversion to bypass degraded links.	Request to change the clause to "The NMS solution should support bandwidth monitoring for specific links to identify bottlenecks during peak hours , with alerting capabilities. Additionally, it should provide capacity planning	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Requirements)		and predictive analysis reports.		of work, functional aspects, supportive technical language for better understanding.
932	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Real-time bandwidth optimization across network segments.	Request to change the clause to "The NMS should support bandwidth monitoring to identify bottlenecks during peak hours and generate alerts when utilization exceeds predefined thresholds.	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
933	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Failure impact analysis for planned maintenance and service continuity.	Request to change the clause to "The NMS should support defining dependencies, displaying live congestion, and automatically creating incidents upon threshold breaches."	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Pls refer preceding response
934	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Detecting and mitigating network congestion with traffic engineering.	Request to change the clause to "The NMS should detect congestion , generate alert incidents, and automatically assign them to the network engineer for resolution."	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
935	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Path computation and optimization	Request to remove this clause as this is not the NMS feature/function	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Pls refer preceding response
936	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target.	Request to remove this clause as this is not the NMS feature/function	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
937	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	The proposed solution should be able to clearly visualize the Hop- by-Hop visibility of the Underlay Network at a granular level Sub- Second) for Identifying clear problematic sections on the Glass pane view	Request to change the clause to "The NMS should detect congestion , generate alert incidents, and automatically assign them to the network engineer for resolution." Ultimate objective is to achieve functionality	This functionality is not a standard NMS feature, To ensure effective congestion management and incident resolution, the clause should be amended to require NMS to detect congestion, generate alerts, and automatically assign incidents to network engineers.	Pls refer preceding response
938	50	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Proposed solution should follow the standard Large IP network industry template from customer order generation to service provisioning. Activation to Billing and accounting to SLA management etc. It should cover each and every steps/stage in between the entire cycle irrespective of whether it is explicitly mentioned or not. These systems should be the one and only systems to manage the entire business of the GFGNL which ultimately fulfill the desires of self-	We are requesting you to modify as :The NMS shall have API to integrate with BSS and other systems and should complete the entire cycle.	NMS can integrate with OSS/BSS tools from different vendors using northbound APIs, ensuring better interoperability and functionality. Therefore, it is recommended to amend the compliance of the RFP accordingly.	At GFGNL, Concept of OVP is to provide the functionality of NMS, OSS and BSS with asked minimum specifications.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			sustainability and embarking on growth path to become most successful Large IP network in the state of Gujarat.			
939	51	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Helpdesk & Customer Issue Management & Problem Management)**	Advanced analytics tools for Pain Value Analysis, Risk Assessment, and Risk Mitigation Planning of TTs	Request to change the clause to "The NMS should Monitors bandwidth usage, congestion points, and resource utilization to predict and prevent potential failures of risk to the network."	This functionality is not a standard NMS feature.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
940	51	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Helpdesk & Customer Issue Management & Problem Management)**	Failure Mode and Effects Analysis	Request to change the clause to "The NMS should monitor congestion and their dependencies and visualizing It for better network analysis and management."	This functionality is not a standard NMS feature.	Pls refer preceding response
941	51	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Helpdesk &**	Provide an option to announce workarounds and solutions to stakeholders efficiently.	Request to change the clause to "The NMS should include an integrated knowledge base to enhance troubleshooting and decision-making."	An integrated knowledge base in NMS enhances troubleshooting and decision-making, making it essential to amend the RFP clause accordingly.	We have mentioned broad functional requirement

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Customer Issue Management & Problem Management)				
942	53	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Performance Management)**	Dynamic link and tunnel delay information.	Request to change the clause to "The NMS should support latency monitoring, round-trip time measurement, and packet analysis for enhanced network performance of the links and tunnels."	This functionality is not a standard NMS feature and may be specific to certain vendors. Therefore, it is recommended to amend the compliance of the RFP accordingly.	Pls refer preceding response
943	54	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+	Infrastructure metrics and logs must be tightly integrated into a single consolidated console for managing infrastructure and security events.	Request to change the clause to "The solution should support infrastructure monitoring with centralized log analysis for improved visibility	Centralized log analysis enhances infrastructure monitoring by improving visibility and issue resolution, making it essential to amend the RFP compliance accordingly.	We have mentioned broad functional requirement

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Network visibility): **(Unified Console)**		and issue resolution."		
944	27	**3.1.1 Eligibility Criteria: Point-5**	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project please refer the definition mentioned above .	Request you to amend this clause for maximum participation and modify it to 2 clients of similar projoect in large ISP, PSU/Govt and BFSI sector. This will bring more technically and competitve OEM to the said bid.	To maximize participation from MII OEMs, an amendment to the RFP compliance is necessary.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
945	31	**3.2.1 Technical qualification criteria, Point-3**	Demonstration of prototype/readiness to meet technology led Governance in NMS and OSS a) Service provisioning automation level b) Network scanning and KPIs c) Digital SLA measurement d) Dashboard for MD, HQ, District, Client e) High performance architecture for speedier reports and real time calculations. f) Integration convenience/understanding as per telco practice by API/NE of all type of elements in BharatNet. g) Any other important functionality to be shown. h) The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 network elements in any Government, PSU, Bank/ pubic listed company or large-scale IP network- 5 Marks	We are requesting to amend and change this clause to demonstrate support fo 15000 network elements in large ISP or Government or bank or PSU for maximum particiaption from MII OeM. We are recommending Make in India OEM and well recognised and establised in NMS domain. This will bring technically, qualified OEM to the bid and bring healthy competition to the said bid.	To maximize participation from MII OEMs, an amendment to the RFP compliance is necessary.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
946	31	**3.2.1 Technical qualification criteria, Point-5**	d) The solutions of OEM must provide at least one reference case demonstrating support for more than **50,000 Customers** in any Government, PSU, Bank/ pubic listed company or large-scale IP network. Presentation to be done for Education department live connections- 3 Marks	Request to amend the clause for atleast one reference case demonstarting support for 15000 Customer instead of 50000 Customer in any Govt/PSU/Public listed company or telecom sector. Allowing established and recognised Make In India OEM will bring more competition.This does not restrict any OEM to participate in the said bid if the criteria will be relaxed. The clause will go against the Make In India OEM who has been established with Govt and Telecom sector for more than 5 years and having support network elements for 15000 Customer. Make in India OEM will loose	To maximize participation from MII OEMs, an amendment to the RFP compliance is necessary.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				the technical points if not considered		
947	**27**	**SECTION-3 EVALUATION CRITERIA 3.1.1 Eligibility Criteria:**	4. The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation	**Kindly amend this clause as:** 4. The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India of value specified herein: **a) One project with the value of at least 40 crores** **b) Two projects, each with the value of at least 30 crores** **c) Three projects, each with the value of at least 20 crores** Similar Project is	The mentioned criteria are specific to networking project which is restricted to participate to get more bid. We request to kindly allow the experience from setup of DC/DR in that network monitoring is the part of project therefore we request to kindly amend this clause.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or **ICCC or** Data Centre having (compute, storage, Security and Networking components) **as a part of the Project.**		
948	**30**	**SECTION-3 EVALUATION CRITERIA 3.2.1 Technical qualification criteria**	The bidder should have supplied, implemented and managed following projects in past 5 years. a) NOC (Network Operation Center)- 3 Marks b) Data center- 3 Marks c) NOC, Data center, (NMS/OSS or Network GIS)- 9 Marks	**Kindly amend this clause as:** The bidder should have supplied, implemented and managed following projects in past. **a) NOC (Network Operation Center)/ICCC- 3 Marks** b) Data center- 3 Marks **c) NOC/ICCC, Data center- 9 Marks**	The mentioned criteria are specific to networking project which is restricted to participate to get more bid. We request to kindly allow the experience from setup of DC/DR in that network monitoring is the part of project therefore we request to kindly amend this clause.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
949	**118**	5.41 Delivery Timeline & Payment	3. Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP - T+5 week- 10% of the total Project Value 4. Delivery of Hardware for IT Infra and Network infra- T + 6 Weeks - 20% of the total Project Value 5. Demonstration of finished software for GFGNL on Bidder's cloud- T + 10 week- 10% of the total Project Value 7. a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru - T + 15 Weeks - 20% of the total Project Value b. Successful completion of FAT, completion of training and Go-live- T + 17	**Kindly amend this cluase as:** 3. Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP - T+5 week- 10% of the total Project Value 4. Delivery of Hardware for IT Infra and Network infra- T + 6 Weeks - **50% of the total Project Value** 5. Demonstration of finished software for GFGNL on Bidder's cloud- T + 10 week- 10% of the total Project Value 7. a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per	As we are submitting 5% PBG for Operation & Maintenance period, Equated quarterly payment term will increase project finance cost which will impact total costing of the work.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Weeks- 10% of the total Project Value 8. Operation & Maintenance - 7 Years from Go live - 30% of the total Project Value as Equated quarterly payments, after the end of each quarter calculated from Go-Live	Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru - T + 15 Weeks - 20% of the total Project Value b. Successful completion of FAT, completion of training and Go-live- T + 17 Weeks- 10% of the total Project Value		
950	**159**	7.6 Service Levels and Performance Penalty During O&M	**Note:** 3. The penalty cap limit for CAPEX will be maximum to 20% of overall amount discovered in financial table for overall capex amount. And same will be applicable to 20% of overall amount discovered in financial table for overall OPEX amount.	**Kindly amend this cluase as:** 3. The penalty cap limit for CAPEX will be maximum to 10% of overall amount discovered in financial table for overall capex amount. And same will be applicable to 10% of overall	Maximun Capping should be 10% as it impact total costing of the work.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				amount discovered in financial table for overall OPEX amount.		
951	59	2	should support **16x10GbE SFP+ ports, 4x10G SX-SFP+** bypass ports, Dual Power supply & **4TB SSD.**	The RFP clause requests a significantly higher number of 10G interfaces. However, as per our understanding, the architecture requires only 2 x 10G IIL links to be terminated. Additionally, the solution specifies HA for both DDoS and Firewall, which implies the need for crisscross WAN/IIL links to be terminated on the DDoS appliance for seamless failover. For multiple links, it is highly recommended to use a WAN switch to aggregate **all current and future IIL links and**	The DDoS appliance should support 4 x 10G SR and 4 x 40G/100G QSFP+ Ports , including 2 bypass ports and populated WITH SR transceiver , Dual Power Supply and 1.9TB SSD	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				forward traffic to the DDoS appliance via a trunk port. As an industry best practice, it is recommended to terminate the total 20G pipe (2 x 10G IIL) directly to the DDoS appliance using 40G/100G ports. This approach reduces cabling complexities and ensures a WAN architecture that remains agnostic to any future changes in IIL or WAN links. Additionally, 100G/40G ports can be utilized to terminate the aggregate bandwidth on the DDoS appliance. Regarding storage, since logs can be sent to a SIEM or analytics tool, we request a relaxation of the 4TB storage requirement to		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				1.9TB SSD to ensure a level playing field for participation to other OEM.		
952	59	3	Device should support at least **80Gbps** throughput	A 80Gbps request is significantly high. Currently, GFGNL is planning for 20Gbps bandwidth, and even if doubled to 40Gbps, it should be sufficient. However, we recommend considering 50Gbps for mitigation purposes. An 80Gbps requirement	Device should support maximum mitigation throughput minimum 50Gbps and minimum 50M of connections.	Please see acceptance in revision for wider participation and cost optimization/savings.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				appears oversized. We suggest the GFGNL team review and adjust the throughput based on actual needs. In DDoS mitigation, effective throughput is a more critical factor than just box throughput.		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
953	59	8	Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, **Defense Win Nuke**, TCP Error Flag	Defense Win Nuke is specific to a particular OEM, and modern systems are no longer vulnerable to this attack. However, ICMP fragmented packets, which were previously used in such attacks, can now be effectively detected and prevented. Change Requested: Replace '**Defense Win Nuke**' with '**ICMP Fragmented Flood**.'	Refer to https://www.radware.com/security/ddos-knowledge-center/ddospedia/nuke/ . Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, **ICMP frgmented flood**, TCP Error Flag	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.
954	59	18	The solution should support Access control	Schedule policies are a function of the	The solution should support Access control	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			list based on inbuilt GeoIP **with configurable duration**.	downstream firewall. Therefore, we request a relaxation of this clause, as it favors specific OEM features.	list based on inbuilt GeoIP.	
955	60	21	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, **Active-Active using VRRP**	VRRP is a Layer 3 clustering protocol, which requires the DDoS unit to function as a gateway. However, typical DDoS deployments use a drop-in inline mode. Therefore, we recommend removing Active-Active configuration.	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
956	60	23	**The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.**	DDoS equipment only participates in cloud signaling, while traffic re-routing is handled by the downstream router or firewall. This clause favors ADC vendors that include DDoS as a small module, whereas pure DDoS vendors do not have a built-in routing	Kindly remove this Cluase	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				engine.Request to emove this clause to ensure fair participation for all OEMs.		
957	-	Disk Drive Support and Encryption	`	· The storage system should have minimum ~~384GB~~ 512GB Global/Federated Data Cache and Expandable upto 768GB 4 TB memory should be delivered on DRAM; any other device or HDD should not be considered as cache.	Higher cache increase the read performance. Every OEM has it's own architecture , some offer global and some federated, if only global is mentioned here then it will become an OEM specific clause.	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
						intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.
958	-	Disk Drive Support and Encryption	· Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives.		-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
959	-	Disk Drive Support and Encryption	· The proposed storage must support data encryption with day 1.	· The proposed storage must support data encryption at rest and in flight with day 1.	Since data will be backed. Up to other storage , hence for data security reasons request you to add encyption while data is copied to backup storage.	1. The security of data is important criteria. 2. It is the SI responsibility to run and operate asked in the RFP without any security/functional risk concerns as part of the overall objectivity against high payouts to SI. 3.The microscopic addition/combination of functionality related flexibility with intend of wider participation has been accorded to SI for deciding appropriately. 4.The purpose is wider competition and for that general principles have been laid. 5.The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
960	-	Storage	· Storage management software should be able to integrate with Active Directory/ LDAP for user authentication		-	Query not clear
961	-	Storage	· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API	~~· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API~~	~~Please clarify what kind of management system will be integrated , this is OEM specific.~~	The OEM shall provide API for integration and same way other OEM also provide the API. This is very basic ask and standard practice in the industry for standard heterogeneous systems. It is the responsibility of GFGNL to ask other OEM for cooperation.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
962	-	Storage	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, Sub-Lun Data Tiering and other	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, ~~Sub-Lun Data Tiering~~ and other . The storage must support native method to detect, prevent and restore data in case of ransomware attack. Any hardware/software must be offered from day 1.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	Deemed Optional for wider participations 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. Sub-Lun -- to be removed
963	-	Storage	required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity.		-	Pls see previous response
964	-	Remote Replicatio n	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. Any external appliance if needed should be quoted to achieve this functionality.	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. ~~Any external appliance if needed should be~~	This requirement is not for active active replication as. per the RFP specificaiton, if both side will be active then read and write at both ends , hence request you to update this clause. This is favouring one single OEM.	GFGNL is removing the DR related all componants and licenses hence bidders don't require to bid for the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				~~quoted to achieve this functionality.~~		
965	-	Licenses	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, ransomware protection, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
966	-	Licenses	· TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR	~~· TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR~~	Please remove these. Certification	Removed

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
967	-	RFP Document / Setction-4 Technical Specification / 4.15 Enterprise Storage / Page 83	Platform	• Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives.	Change of Clause • Offered Storage array shall be a true flash optimized Hybrid array supporting both **TLC NVMe SSD** drives and spinning drives. Justification TLC NVMe SSDs provide an optimal balance of performance, endurance, and cost efficiency for enterprise storage. They offer high throughput and low latency with the NVMe interface, ensuring fast data access. Compared to other SSD types, TLC technology is cost-effective while maintaining excellent reliability and endurance for mixed workloads. Additionally, modern enterprise-grade TLC SSDs feature advanced wear leveling and error correction, making them suitable for sustained performance in hybrid storage environments. This specification ensures	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					an efficient, scalable, and cost-optimized storage solution.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
968	-	RFP Document / Setction-4 Technical Specification / 4.15 Enterprise Storage / Page 84	Investment Protection with Virtualization	Offered Storage array shall support heterogeneous storage virtualization natively for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage.	Addition of Clause Offered Storage array shall support heterogeneous storage virtualization natively for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. Justification Including storage virtualization in storage specifications enhances resource utilization and simplifies management by providing centralized control over multiple devices. It offers flexibility and scalability for easy expansion, improves data protection through efficient backup and recovery, and reduces overall costs by maximizing existing hardware. Additionally, it optimizes performance through load balancing	Offered Storage array shall support heterogeneous storage virtualization natively or third-party or other workaround for reputed storage product of similar nature and size without any direct and license cost to the GFGNL as part of delivering the investment protection.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					and supports various storage types, making it essential for modern storage strategies.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
969	-	RFP Document / Setction-4 Technical Specification / 4.15 Enterprise Storage / Page 84	Data Loss	The solutions should ensure zero data loss (OEM need to provide assurance in the MAF)	Query 1. Please specify, zero data loss has to be achieved without a need of configuring replication. Justification To achieve zero data loss with replication 3 different sites are required with combination of sync and async replication. Which required a lot of investment on 3 sites. So zero data loss without replication provide cost effective solution and ensure data availability in any failure scenario.	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
970	-	RFP Document / Setction-4 Technical Specification / 4.16 Backup Storage / Page 87	Investment Protection with Virtualization	Offered Storage array shall support heterogeneous storage virtualization natively for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage.	Addition of Clause Offered Storage array shall support heterogeneous storage virtualization natively for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. Justification Including storage virtualization in storage specifications enhances resource utilization and simplifies management by providing centralized control over multiple devices. It offers flexibility and scalability for easy expansion, improves data protection through efficient backup and recovery, and reduces overall costs by maximizing existing hardware. Additionally, it optimizes performance through load balancing	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					and supports various storage types, making it essential for modern storage strategies.	
971	-	RFP Document / Setction-4 Technical Specification / 4.16 Backup Storage / Page 87	Data Loss	The solutions should ensure zero data loss (OEM need to provide assurance in the MAF)	Addition of Clause The solutions should ensure zero data loss (OEM need to provide assurance in the MAF) Justification This cluase has part of Enterprise storage technical specification, but missing in backup storage specification.	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					Backup storage is also equally important for the infrastructure. Please add this parameter in backup storage technical compliance.	
972	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software cost) / Page 164	Virtualization software	Query Virtulization software qty is mentioned as 1. This 1 Virtualization software is required for DC site? DR requirement is not mentioned anywhere.	Query Virtulization software qty is mentioned as 1. This 1 Virtualization software is required for DC site? DR requirement is not mentioned anywhere.	GFGNL is removing the DR related all components and licenses hence bidders don't require to bid for the same.
973	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID	Server	Query Server or virtulization requirements for DR site are not mentioned anywhere. Please specify.	Query Server or virtulization requirements for DR site are not mentioned anywhere. Please specify.	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		FORMAT / PART-A (Hardware & Software cost) / Page 164				
974	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software cost) / Page 164	Backup Server	Query 2 Qty of backup servers are requested in the requirement. How these 2 servers will be utilized ? Will there be a cluster configurd on these servers ?	Query 2 Qty of backup servers are requested in the requirement. How these 2 servers will be utilized ? Will there be a cluster configurd on these servers ?	Pls see previous response
975	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software	Enterprise Storage	1+1	Query 1+1 Enterprise storage is required for DC site or It is the requirement for DC and DR storage? Becuase DR storage requirement is not mentioned anywhere.	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		cost) / Page 164				
976	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software cost) / Page 164	Backup software for storage	Query Is this Perticular is Backup storge ? Because Backup storage technical specifications are available in technical specifications but requried quantity is not mentioned in finantial bid format.	Query Is this Perticular is Backup storge ? Because Backup storage technical specifications are available in technical specifications but requried quantity is not mentioned in finantial bid format.	Pls see revision
977	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software	DR Rsources		Query/Addition of Clause To configure and optimize the DR site resouces, please specify complete list or % requirement of resources at DR.	GFGNL is removing the DR related all componants and licenses hence bidders don't require to bid for the same.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		cost) / Page 164				
978	-	RFP Document / Setction-8 FINANCIAL BID / FINANCIAL BID FORMAT / PART-A (Hardware & Software cost) / Page 164	SAN Switch	2+2	Addition of Clause SAN switch requirement is not mentioned anywhere in the Finantial Bid format. Please add required quantity of SAN switch for DC and DR site. Justification SAN switches are assential for any expansion in number of servers in the future. Redundant SAN switches at each site is a architetural best practice.	Appropriate SAN switch or any other requirement for completeness of the solution with specified performance, capacity, ports mapping and etc is in overall responsibility of SI as part of full scale solution without any additional cost to GFGNL.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
979	-	RFP Document / Setction-4 Technical Specification / 4.14 Server / Page 81	HBA Card	64 Gbps Host Bus Adaptor for connecting to SAN Switch with Storage	Clarification 1. The HBA card usually has 2 x 32 Gbps Ports. So the aggregate bandwith of Host Bus Adaptor is 64 Gbps. So in this point you need aggregate bandwith or a single port running 64 Gbps. Note: All other component specifications mentions 32 Gbps FC connections. 2. SAN switch specificationsand requirement are not mentioned anywhere in the technical specifications. Please clarify on that. SAN switches are assential for any expansion in number of servers in the future.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
980	-	RFP Document / Setction-4 Technical Specification / 4.13 Virtualization solution / Page 78	Virtualization software should have the ability to live migrate Virtual machines files from one storage array to another without any Virtual Machine downtime. It should support this migration from one storage protocol to another (ex. FC, iSCSI, NFS, DAS-all of these)	NA	Change of Clause The virtualization platform should support live migration of virtual machines within a shared storage environment. For migrations across different storage protocols, the platform should provide mechanisms for storage replication and workload failover to ensure seamless data movement without application disruption. Justification Cross-protocol live migration is not an industry-standard practice due to differences in storage architectures, access methods, and performance characteristics, which can cause data integrity issues and downtime risks. A more reliable approach is to use storage replication and failover mechanisms, ensuring seamless data	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					transitions without disrupting workloads. This method aligns with modern cloud-native principles, improves stability, and enhances scalability, making it a more efficient and resilient alternative to hypervisor-driven cross-protocol migration.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
981	-	RFP Document / Setction-4 Technical Specification / 4.13 Virtualization solution / Page 78	Hypervisor platform shall be able to detect the hardware conditions of the host node and shall proactively evacuate the Virtual machines before the hardware issues cause an outage to Virtual machines thus ensuring high availability.	NA	Change of Clause The virtualization platform should be able to detect hardware condition or support integration with external infrastructure monitoring tools to assess hardware health. Based on these insights, it should allow for automated workload migration or failover mechanisms to minimize disruption in case of hardware issues. Justification Hardware failure detection is best handled by dedicated infrastructure monitoring tools rather than the hypervisor, as these tools provide deeper vendor-specific insights and proactive alerts. Relying solely on the hypervisor for failure detection may lead to unnecessary VM evacuations and performance degradation. Instead,	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					integrating with external monitoring solutions enables a more efficient and scalable high-availability strategy, ensuring reliable workload migration only when necessary.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
982	-	RFP Document / Setction-4 Technical Specification / 4.13 Virtualization solution / Page 78	Hypervisor shall provide Storage I/O Control for prioritizing storage access by continuously monitoring I/O load of a storage volume and dynamically allocating available I/O resources to virtual machines according to business needs	NA	Change of Clause The virtualization platform should provide mechanisms to optimize storage performance by monitoring I/O load and prioritizing access based on business needs. This can be achieved either through hypervisor-level controls or by integrating with storage solutions that offer QoS-based I/O management to dynamically allocate available resources according to workload demands. Justification Instead of relying on hypervisor-based SIOC the revised clause broaden the approach to include both hypervisor-level and storage-level solutions.It allows flexibility for different IT architectures, whether using hypervisor-driven I/O	Deemed optional. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					management or storage-layer QoS controls (used in modern SDS solutions). This ensures compatibility with various storage strategies while avoiding reliance on a single vendor-specific approach.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
983	-	RFP Document / Setction-4 Technical Specification / 4.13 Virtualization solution / Page 78	Hypervisor shall provide Network I/O Control for prioritizing network access by continuously monitoring I/O load over the network and dynamically allocating available I/O resources according to business needs.	NA	Change of Clause The hypervisor platform should support network traffic prioritization to ensure optimal resource allocation based on workload demands. This can be achieved through hypervisor-driven mechanisms or by integrating with SDN solutions and network QoS policies that dynamically monitor and allocate network resources according to business needs. Justification This revision ensures that both hypervisor-based and network-layer approaches are considered, providing flexibility for organizations to choose the most scalable and efficient method based on their infrastructure.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
984	-	RFP Document / Setction-4 Technical Specification / 4.13 Virtualization solution / Page 78	The virtualization software should provide in-built Replication capability which will enable efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.	NA	Change of Clause The virtualization platform should support efficient replication of virtual machine data across different storage solutions over LAN or WAN. This can be achieved either through in-built replication mechanisms or by integrating with storage and backup solutions that enable array-agnostic replication, allowing flexible RPO policies and simplified management at the virtual machine level. Justification Alowing both builtin and storage and backup solution based replication approch allows businesses to choose the most efficient replication method based on workload requirements. It supports both hypervisor-based and	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					storage/backup-driven replication for flexibility and eliminates vendor lock-in and supports heterogeneous storage environments. This also aligns with modern enterprise disaster recovery (DR) strategies.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
985	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Suggestion:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have built-in bypass as best practice.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
986	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or mitigation capability.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
987	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Suggestion:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.
988	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
989	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	**Hence requesting you to remove this point.**	**Suggestion:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
990	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	**Hence requesting you to remove this point.**	**Suggestion:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
991	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Suggestion:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
992	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Suggestion:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
993	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Suggestion:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
994	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Suggestion:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
995	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Suggestion:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
996	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					sophisticated flood attacks.	
997	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Suggestion:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
998	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT	**Suggestion:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	
999	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Suggestion:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user productivity and business.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1000	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance	**Suggestion:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				for SSL TPS scalability		
1001	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	**Suggestion:** DDoS solution should have capability to detect and mitigate different protocol attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1002	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Suggestion:** For service provider kind of customer, it is recommended to have solution deployed out-of-path for reduced latency.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1003	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Suggestion:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1004	-	4.4 DDoS - Distribute	Additional Clause	Proposed OEM should be deployed and used by at least	Proposed OEM should be deployed and used by at least 2 Tier-1	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		d Denial-of-Service		2 Tier-1 service providers for DDoS mitigation in India	service providers for DDoS mitigation in India	
1005	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Suggestion:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1006	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Suggestion:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1007	29	3.1.1 Eligibility Criteria	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 / TL9000 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	We Request department to kindly consider TL9000 certification in place of ISO9001. TL9000 encompasses all the requirements of ISO9001, ensuring compliance with the same standards. Additionally, the issuing authority for both certifications is the same, i.e., BSI. Which further validates its credibility and alignment with ISO standards.	Repeated queries

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1008	129	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation :	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation: Security is paramount. The bidder will be responsible for planning of IT security policy and require to create security posture for all the ICT infrastructure of GFGNL. Not limited to that bidder has to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) for the GFGNL Cloud and all network components of GFGNL network components which will includes the Amendment BharatNet program and other consecutive Phases. All software requirement to perform VAPT will be the scope of bidder and additionally, the bidder must facilitate a third-party security audit as and when performed by GFGNL or authorized agency and hardening for critical devices to ensure the security of the	What is the expected frequency for conducting Vulnerability Assessment and Penetration Testing (VAPT)	-	1. The design of security architecture, supply of quality and reputed products for running the NOC in a secured manner is the prime responsibility of capable bidder. As part of the scope of work, we have indicated security products with high payouts to successful bidder for security compliances including quarterly VAPT for proactive and preventive measures in the larger interest of fulfillment of purpose of NOC. The bidders are advice to do proper due diligence while choosing security products. 2. It is expected that bidder shall design and implement security architecture and shall be expert to derive security strength of the product, writing scripts for preventions and ability to run and manage the underlaying network of Bharatnet and NOC components efficiently in most secured manner with best of security practices.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			infrastructure. Bidder has to resolve all the vulnerability within stipulated time and need to consider CVSS 3.0 and the latest scoring for severity need adhere in operation and maintenance phase (i.e. 7 + 3 years). Severity category and resolution time has been provided in the VAPT penalty section 7.11 of this RFP and need to resolve all the potential vulnerabilities. Security team has to ensure all the necessary postures are updated in the GFGNL environment			

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1009	129	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation :	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation: Security is paramount. The bidder will be responsible for planning of IT security policy and require to create security posture for all the ICT infrastructure of GFGNL. Not limited to that bidder has to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) for the GFGNL Cloud and all network components of GFGNL network components which will includes the Amendment BharatNet program and other consecutive Phases. All software requirement to perform VAPT will be the scope of bidder and additionally, the bidder must facilitate a third-party security audit as and when performed by GFGNL or authorized agency and hardening for critical devices to ensure the security of the	Could GFGNL provide further details on the expected deliverables for the IT Security Policy?	-	1. The design of security architecture, supply of quality and reputed products for running the NOC in a secured manner is the prime responsibility of capable bidder. As part of the scope of work, we have indicated security products with high payouts to successful bidder for security compliances including quarterly VAPT for proactive and preventive measures in the larger interest of fulfillment of purpose of NOC. The bidders are advice to do proper due diligence while choosing security products. 2. It is expected that bidder shall design and implement security architecture and shall be expert to derive security strength of the product, writing scripts for preventions and ability to run and manage the underlaying network of Bharatnet and NOC components efficiently in most secured manner with best of security practices.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			infrastructure. Bidder has to resolve all the vulnerability within stipulated time and need to consider CVSS 3.0 and the latest scoring for severity need adhere in operation and maintenance phase (i.e. 7 + 3 years). Severity category and resolution time has been provided in the VAPT penalty section 7.11 of this RFP and need to resolve all the potential vulnerabilities. Security team has to ensure all the necessary postures are updated in the GFGNL environment			

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1010	129	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation :	6.2.10 ICT Security, Policy, VAPT & Risk Mitigation: Security is paramount. The bidder will be responsible for planning of IT security policy and require to create security posture for all the ICT infrastructure of GFGNL. Not limited to that bidder has to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) for the GFGNL Cloud and all network components of GFGNL network components which will includes the Amendment BharatNet program and other consecutive Phases. All software requirement to perform VAPT will be the scope of bidder and additionally, the bidder must facilitate a third-party security audit as and when performed by GFGNL or authorized agency and hardening for critical devices to ensure the security of the	Does the bidder have to provide third-party security audit in the Solution Could GFGNL provide a list of critical devices that require hardening?	-	1. The design of security architecture, supply of quality and reputed products for running the NOC in a secured manner is the prime responsibility of capable bidder. As part of the scope of work, we have indicated security products with high payouts to successful bidder for security compliances including quarterly VAPT for proactive and preventive measures in the larger interest of fulfillment of purpose of NOC. The bidders are advice to do proper due diligence while choosing security products. 2. It is expected that bidder shall design and implement security architecture and shall be expert to derive security strength of the product, writing scripts for preventions and ability to run and manage the underlaying network of Bharatnet and NOC components efficiently in most secured manner with best of security practices.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			infrastructure. Bidder has to resolve all the vulnerability within stipulated time and need to consider CVSS 3.0 and the latest scoring for severity need adhere in operation and maintenance phase (i.e. 7 + 3 years). Severity category and resolution time has been provided in the VAPT penalty section 7.11 of this RFP and need to resolve all the potential vulnerabilities. Security team has to ensure all the necessary postures are updated in the GFGNL environment			
1011	142	6.6 Manpower requirement on Payroll of SI (No Subcontra	6.6 Manpower requirement on Payroll of SI (No Subcontracting is allowed):	Request GFGNL allow Subcontracting	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		cting is allowed):				
1012	26	3.1.1 Eligibility Criteria	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	The bidder should have average annual turnover of minimum INR 500 Crores in last three financial years as on 31st March 2024.	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1013	27	3.1.1 Eligibility Criteria	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company or **Private Enterprises** in India during past Seven years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as:	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			components) and managing, monitoring network nodes as a part of the Project.	Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.		
1014	49	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):2 Functional Requirement	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing . However to achieve the path tracing between GP to NOC and GP to Internet OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.	By deploying the testing agents will help perform monitorng the the Network based KPIs like Packet loss,latency,jitter	The functional specification has been specified. It is the SI responsibility to provide the same

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1015	51	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):4 Network Topolozy and Visulaization	Network path visualization: a time-correlated, unified view of all paths between any two points on network. With visibility across network, application, routing, and device layers.	To get the network path visualization deploying light weight software/hardware based testing agents is allowed and ICMP/TTL propagation is enabled .	By deploying the testing agents will help monitor the Network path and get the visualizations of paths.	Pls refer preceding response
1016	52	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): 6 Network scanning	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing . However to achieve the path tracing between GP to NOC and GP to Internet OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.	By deploying the testing agents will help perform monitorng the the Netwokr based KPIs like Packet loss,latency,jitter	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1017	135	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 3	The proposed solution should support synthetic network test at both ends of a monitored path (GP to S-NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput–an improved form of the bandwidth metric–along with Path Visualization and path MTU.	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing . However to achieve the path tracing between GP to NOC and GP to Internet OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.	By deploying the testing agents will help perform monitorng the the Netwokr based KPIs like Packet loss,latency,jitter	Pls refer preceding response
1018	135	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 1	The Proposed solution should have an architecture supporting ease of deployment, zero touch maintenance and seamless monitoring could be on premise or MeitY empaneled cloud based.	The word should be rewritten as "The Proposed solution should have an architecture supporting ease of deployment, zero touch maintenance and seamless monitoring could be on premise or may be on empaneled/**secured** cloud based.	-	Ask related to cloud/ related provisions is optional for wider participation.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1019	136	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 9	Real time visibility & monitoring of both Network and Application(s) for better co-relation of the Service impact pro-actively rather than re-actively. (Milli Second Level visibility: 20pps to 1000 pps for real time monitoring) for continuous real time KPIs and SLA reporting.	Pls modify this as follows " (Milli Second Level visibility: 10pps to 100 pps for Near real time monitoring)	If the traffic is sent with higher number of pps to target servers/link which might face some rejection from target servers which will affect the monitoring of services.	Allowed
1020	136	23. Network Element Management System - > 24.> c) Service Performance Monitoring (Qualitative Service Visibility): 16	Additional Point	Solution shall support deploying l ightweight, software-based agents to monitor key internal or cloud-based applications and services.	Testing methodology	Pls refer preceding response
1021	136	23. Network Element Management System - > 24.> c)	Additional Point	Solution shall provide easy sharing of interactive monitoring views to aid internal teams and external providers and	Keeping transperancy while sharing the data	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Service Performance Monitoring (Qualitative Service Visibility): 17		vendors to collaborate to solve problems fast.		
1022	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Justification:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have built-in bypass as best practice.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1023	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				mitigation capability.		
1024	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Justification:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.
1025	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack	Requesting you to Plesae remove this point.	**Justification:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**,	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			protection features from the day of installation		however LLB is a stateful device. This is relevant for DDoS solution	
1026	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	Requesting you to Plesae remove this point.	**Justification:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1027	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	Requesting you to Plesae remove this point.	**Justification:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1028	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Justification:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1029	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Justification:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1030	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Justification:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1031	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Justification:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1032	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Justification:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1033	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Justification:** DDoS solution should have capability to detect and mitigate different types of	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					sophisticated flood attacks.	
1034	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Justification:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1035	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	**Justification:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
1036	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Justification:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					productivity and business.	
1037	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance for SSL TPS scalability	**Justification:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1038	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	Justification: DDoS solution should have capability to detect and mitigate different protocol attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1039	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Justification:** For service provider kind of customer, it is recommended to have solution deployed out-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					of-path for reduced latency.	
1040	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Justification:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1041	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should be deployed and used by at least 2 Tier-1 service providers for DDoS mitigation in India	Proposed OEM should be deployed and used by at least 2 Tier-1 service providers for DDoS mitigation in India	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1042	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Justification:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1043	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Justification:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1044	81	System Memory	Min 768 GB DDR-5 or Latest, supported up to 4 TB or higher with 24 or more DIMM slots; ECC Advance	Kindly modify the clause as "Min 768 GB DDR-5 or Latest, supported up to 4 TB or higher with 24 or more DIMM slots; ECC"	Kindly modify for wider participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1045	81	Server Interface	Serial Port, 2 x USB 3.2 Gen 1Port,	kindly modify the clause as "-Serial Port, 2 x USB 3.0/3.2 Gen 1 Port,"	Kindly modify for wider participation as both have same transfer speeds.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1046	82	System Security	Secure erase of NAND/User data	Kindly modify as "Secure Erase"	Kindly modify the clause as its OEM specific	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1047	-	Server Security Features-2	Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.	Kindly ammend it as "" Solution should support firmware rollback	The current clause is OEM specific. Every OEM have different architecture for firmware rollback. Kindly amend the clause to qualify and wider participation."	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1048	89	Backup Server Interface	2 x USB 3.2 Gen1 ports or higher	kindly modify the clause as " 2 x USB 3.0/3.2 Gen 1 Port or higher,"	Kindly modify for wider participation as both have same transfer speeds.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1049	90	Backup server System Security	Secure erase of NAND/User data	Kindly modify as "Secure Erase"	Kindly modify the clause as its OEM specific	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1050	90	Backup Firmware security	Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	Kindly ammend it as "Solution should support firmware rollback"	The current clause is OEM specific. Every OEM have different architecture for firmware rollback. Kindly amend the clause to qualify and wider participation."	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1051	91	Backup server Embedded Remote Management and firmware security	Server should support storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware.	Kindly ammend it as " Solution should have remote management to manage repository for firmware, drivers, and software components "	The current clause is OEM specific. Every OEM have different architecture for remote management. Kindly amend the clause to qualify and wider participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1052	91	Backup server Embedded Remote Management and firmware security	Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation.	Kindly modify the clause as "Remote console sharing up to 2 users simultaneously during pre-OS and OS runtime operation."	Current clause is OEM specific, For wider participation, kindly modify the clause.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1053	57	4.3 Network Intrusion Prevention System (NIPS) / 2	• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 140Gbps on the same box (1 RU) supporting 60M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL.	The organization's network size and growth rate do not necessitate stacking to achieve 400 Gbps. Also a single appliance can handle the network's throughput requirements upto 140Gbps. The latency parameter can change based on multiple parameters like type of port , bandwidth , security configurations in the solution , load on the solution etc. therefore necessiate the changes.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1054	58	4.3 Network Intrusion Prevention System (NIPS) / 3	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure.	Should be an on-premise standalone NIPS appliance.	Please consider the changes as this blocks many security vendors like us to participate .	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1055	63	4.6 Next Generation Firewall /2	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active, Active/Passive and HA clustering support.	The firewall should have minimum 4 x100/40G,4x10G/25G and 4 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active (HA clustering support) and Active/Passive.	The changed interface density will suffice the requirement. It will not affect the overall ask.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1056	63/64	4.6 Next Generation Firewall /2	• The Appliance must handle the threat prevention throughput of minimum 60 Gbps enabling security features and measured with Enterprise Mix /Application Mix traffic. • The Firewall must deliver minimum 80 Gbps of IPSEC throughput from day 1.	• The Appliance must handle the threat prevention throughput of minimum 100 Gbps scalable upto 140 Gbps enabling security features and measured with Enterprise Mix /Application Mix	The threat prevention throughput asked is quite low with respect to the concurent session asked, hence increasing it. Also reducing the new connection per second to 800K with AVC enable The throughput	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			• The Appliance should support minimum New Connections per Sec of 1 million. • The Application should have Concurrent Sessions of – 60 million from day one.	traffic. • The Firewall must deliver minimum 80 Gbps of IPSEC throughput from day 1. • The Appliance should support minimum New Connections per Sec of 800K with AVC. • The Application should have Concurrent Sessions of – 60 million from day one.	will also go in sync with NIP's.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1057	64	4.6 Next Generation Firewall / 5	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window can be schedule or automatic** **• Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV action such as allow, deny/drop,alert etc.** **• NGFW should have**	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware/IPS signatures and should have minimum signatures update**	CDR is a functionality of email security solution and this can be achieved using email security in conjunction of NGFW which are specialized for content sanitization. This is not a primary focus of firewall. SSH inspection causes SSH traffic , breaks the connection and causes issues in regaining connection.There is no specific use case of SSH inspection. These are all specific to OEM, kindly update the changes for better particiation and with the changes suggested the functional requirement remains same.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time. **• IPS must deliver more than 10000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect against Denial of Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces	**window can be schedule or automatic** **• Should be able to perform Anti-virus /IPS scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV/IPS action such as disable, deny/drop,alert etc.** **• NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time.** **• IPS must deliver more than 20000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			policies with various categories and ability to queries a real time OEM threat intel database • **The NGFW should have both SSL and SSH Inspection capabilities"**	against Denial of Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies with various categories and ability to queries a real time OEM threat intel database • **The NGFW should have both SSL or SSH Inspection capabilities"**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1058	76	4.12 AAA Server/ 5	AAA Solution should be scalable enough to support added endpoints in the network. Facility to integrate with multiple devices and gateways i.e SMS, Payment, Email ..etc.	AAA Solution should be scalable enough to support added endpoints in the network. Facility to integrate with multiple devices and gateways i.e SMS, Email ..etc.	For a NAC, there won't be a use case for payment as a gateway. Please remove the same.	The AAA (Authentication, Authorization, and Accounting) server is required to authenticate NOC users securely, ensuring controlled access based on predefined roles and policies. The solution must support integration with multiple authentication methods, including LDAP, RADIUS, TACACS+, and multi-factor authentication (MFA), to enhance security. Additionally, audit logs should be maintained for compliance and monitoring purposes.
1059	159	Penalty	3. The penalty cap limit for CAPEX will be maximum to 20% of overall amount discovered in financial table for overall capex amount. And same will be applicable to 20% of overall amount discovered in financial table for overall OPEX amount. 4.The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 20% of Total Quarterly Payable. The penalties, if any, will be recovered against the quarterly payment invoice submitted by the agency. If the penalty exceeds for the two consecutive Quarter, then notwithstanding anything contained herein, the	Would request you to cap Max penalty to 10% instead of 20%.	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Purchaser may take appropriate action including the termination of the contract and forfeiting of the Performance Guarantee			
1060	164	FINANCIAL BID FORMAT	Any other components inadvertently missed out but require for overall solution and for compliance of RFP and GOG/GOI guidelines	Would request you to help in sharing exhaustive list for the same as it can creates issues while submission commercials as other Bidder might or not consider those items which might require.	-	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
1061	15	Fact Sheet, Point 12	Bid Security/ Earnest Money Deposit (EMD) - on Account	We request you to allow submission of EMD in the form of Bank Guarantee & DD also.	Since the EDM Amount is in Crores, please allow to submit BG also.	To be taken from PH-III Query
1062	27	3.1.1 Eligibility Criteria: Point 4	Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having	I	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			(compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.			
1063	28	3.1.1 Eligibility Criteria: Point 4	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	We request to revise this clause as The Bidder must possess all the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	For better service quality.	This seems suggestion of eliminating others.
1064	118	5.41 Delivery Timeline	Submission of PBG= T + 3 weeks	Submission of PBG= **T + 6 weeks**	-	As per RFP
1065	118	5.41 Delivery Timeline	a. Project Kick-off b. Technical architecture – IT Infra c. Technical architecture – Network infra d. Configuration of functional requirement of software GIS and NMS on bidders cloud as per RFP Solution. Design Document	a. Project Kick-off b. Technical architecture – IT Infra c. Technical architecture – Network infra d. Configuration of functional requirement of software GIS and	We request to allow sufficient time for these activities.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			with detailed HLD, LLD, Deployment Plan, Testing Plan, Risk Management Plan, Change management plan, O&M Plan, etc. -------- T + 3 weeks	NMS on bidders cloud as per RFP Solution. Design Document with detailed HLD, LLD, Deployment Plan, Testing Plan, Risk Management Plan, Change management plan, O&M Plan, etc. -------- **T + 6 weeks**		
1066	118	5.41 Delivery Timeline	Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP = T + 5 weeks	Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP **= T + 8 weeks**	-	As per RFP
1067	118	5.41 Delivery Timeline	Delivery of Hardware for IT Infra and Network infra = T + 6 weeks	Delivery of Hardware for IT Infra and Network infra = **T + 12 weeks**	-	As per RFP
1068	118	5.41 Delivery Timeline	a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru = T + 15 weeks	a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru = **T + 24 weeks**		
1069	119	5.41 Delivery Timeline	Supply, Installation, integration, Testing and FAT of field components as per scope at each location.	**8 Weeks** from the date of order issued to agency.	-	As per RFP
1070	118	**Delivery Timeline & Paymentv Term**	Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP	10% of the total Project Value	-	As per RFP
1071	118		Delivery of Hardware for IT Infra and Network infra - 20% of the total Project Value	Delivery of Hardware for IT Infra and Network infra - **50% of the total Project Value**	-	As per RFP
1072	118		Demonstration of finished software for GFGNL on Bidder's cloud	10% of the total Project Value	-	As per RFP
1073	118		Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru	10% of the total Project Value	-	As per RFP
1074	118		Successful completion of FAT,	10% of the total Project Value	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			completion of training and Go-live			
1075	119		Operation & Maintenance - 30% of the total Project Value as Equated quarterly payments, after the end of each quarter calculated from Go-Live	**10% of the total Project Value** as Equated quarterly payments, after the end of each quarter calculated from Go-Live	-	As per RFP
1076	119	Delivery Timeline	No advance payment will be made	Please allow 20% Mobilization advance against ABG	For the smooth start of the project	As per RFP
1077	26	Eligibility Criteria	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024	Please consider ICT annual turnover of total smart city project which includes Survillance , ATCS, Data Center and ICCC	Should also consider Survillance , ATCS in ICT scope	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1078	28	Eligibility Criteria	The bidder should: a) Not have been banned / blacklisted by Central Government / Any State Government / PSU in India as on the date of bid submission. b) Not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons. c) Not have their directors and officers convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified.	Please modify clause as below : Not have been banned / blacklisted by Central Government / Any State Government / PSU i**n IT/ ICT business** in India	Most of companies are doing business under one name so this clause should relate to only IT/ICT business.	It is standard clause in public procurement

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1079	29	Eligibility Criteria	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	Please consider the certifications of point b,c and d of Subcontractor/consortium partner	Allow Subcontractor/consortium.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1080	Page 82	**Technical spec**	**4.14**	Point 18, Industry Standard Compliance: • ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3, TLS 1.2, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4. Or any equivalent.	• ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft Logo certifications, PXE Support, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES),SNMP v3, TLS 1.2,DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 Or any equivalent.	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1081	**4**	**Technical**	**4.14 Server**	System Security: UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, BezelLocking Kit option, Support for Commercial National Security Algorithms (CNSA),	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) on browser, Bezel Locking Kit option, Chassis Intrusion detection option	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Chassis Intrusion detection option		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1082	**90**	**Technical**	**Backup server**	• ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3, TLS 1.2, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4. Or any equivalent.	• ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft Logo certifications, PXE Support, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES),SNMP v3, TLS 1.2,DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 Or any equivalent.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1083	**90**	**Technical**	**Backup server**	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms (CNSA), Chassis Intrusion detection option	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) on browser, Bezel Locking Kit option, Chassis Intrusion detection option	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1084	**4**	**Technical**	**4.17 Backup server**	• System remote management should support browser based graphical remote console along with Virtual Power button,	• System remote management should support browser based graphical remote console along	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1085	-	-	**4.17 Backup server**	remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder . • Server should have dedicated 1Gbps remote management port • Server should support storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. Server should support agentless management using the outof-bandremote management port.	with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder. 1 Server should have dedicated 1Gbps remote management port 2 Server should support storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. • 3 Server should support agentless management using the out-of-band remote management port. • 4 Local or Directory-based user accounts with Role based access control. • 5 Remote	Deemed Optional for wider participation and deduplication 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device is well established. The additional functionalities stands optional for unnecessary eliminations. This is performance related deviation. The request of signification downgrading intend is not allowed. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable for wider participation of products including combining functionalities/deduplication for meeting overall business and functionality objectives. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				• Local or Directory-based user accounts with Role based access control. • Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	console sharing up to 6 users simultaneously during pre-OS and OS runtime operation. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	
1086	-	-		• Server should have dedicated 1Gbps remote management port	• Server should have dedicated 1Gbps remote management port	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1087	**27**	**3.1.1 Eligibility Criteria**	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	**The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past 8 years from the date of bid submission of value specified herein:** **a) One project with the value of at least 40 crores with 2.5K network Nodes or** **b) Two projects, each with the value of at least 30 crores with 2K network Nodes or** **c) Three projects, each with the value of at least 20 crores with 1.5K network Nodes**	**In BSNL CNOC Tender eligibility given as below: The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past 10 years from the date of bid submission of value specified .** **This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1088	**27**	**3.1.1 Eligibility Criteria**	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in **past 7 years.** For similar project please refer the definition mentioned above .	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in **past 8 years**. For similar project please refer the definition mentioned above .	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	For wider participation- two clients experience is allowed. Pls see revision
1089	**28**	**3.1.1 Eligibility Criteria**	a) The bidder should be authorized by OEMs of the proposed Product to quote their product or any third-party product to complete the solution as per RFP. b) The bidder should also have a back-to-back support agreement/arrangement with OEMs for after sale support & services including supply of spare parts etc. The proposed product quoted in the bid should not be declared EOL or EOSS for next 7 Years from the date of Bid Submission.	a) The bidder should be authorized by OEMs of the proposed Product to quote their product or any third- party product to complete the solution as per RFP. b) The bidder should also have a back-to-back support agreement/arrangement with OEMs for after sale support & services including supply of spare parts etc. **The proposed product quoted in the bid should not**	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	Since Project duration is more 7+3 years. GFGNL is affirming that deployed product must serve with full support and demanding from the bidders for the duration.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				be declared EOL or EOSS for next 5 Years from the date of Bid Submission.		
1090	**28**	**3.1.1 Eligibility Criteria**	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 **b) ISO/IEC 14000-1:2018** c) ISO/IEC 27001:2022 **d) ISO/IEC 45000-1:2018**	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.** **ISO/IEC 20000-1:2018 certification we will provide after 6 months of the award of contract.**	As per RFP
1091	**118**	**5.1 Delivery Timeline**	Delivery of Hardware for IT Infra and Network infra- T + 6 Weeks -20% of the total Project Value	Delivery of Hardware for IT Infra and Network infra- **T + 10 Weeks -40% of the total Project Value**	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1092	**118**	**5.1 Delivery Timeline**	Demonstration of finished software for GFGNL on Bidder's cloud T + 10 Weeks -10% of the total Project Value	Demonstration of finished software for GFGNL on Bidder's cloud **T + 12 Weeks** -10% of the total Project Value	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	As per RFP
1093	**118**	**5.1 Delivery Timeline**	a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharat net S-NOC (C-S-NOC) at New Delhi & Bengaluru T + 15 Weeks -20% of the total Project Value b. Successful completion of FAT, completion of training and Go-live T + 17 Weeks -10% of the total Project Value	a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharat net S-NOC (C-S-NOC) at New Delhi & Bengaluru **T + 17 Weeks -10% of the total Project Value** b. Successful completion of FAT, completion of training and Go-live **T + 19 Weeks -10%**	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				of the total Project Value		
1094	**119**	**5.1 Delivery Timeline**	Operation & Maintenance 7 Years from Go live 30% of the total Project Value as Equated quarterly payments, after the end of each quarter calculated from Go-Live	Operation & Maintenance 7 Years from Go live **20% of the total Project Value as Equated quarterly payments, after the end of each quarter calculated from Go-Live**	**This is considered essential to enable bidders with minimum yet promising experience and expertise to bid for the tender. Else, this clause is restrictive and will limit the number of bids.**	As per RFP
1095	32	3.2.1 : Technical Qualificati on Criteria	Value added offering over and above the ask of RFP without any additional charges. • Use of Licenses, higher capacity in storage/ No of cores, manpower, contract duration, offering of AI and etc. (10 Marks)	The total marks including the marks for clause mentioned here is 110. The sub-total calcuates 100 marks. Can you please clarify it or kindly re-check and correct the marks distribution	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1096	164	Financial Bid Format (Part A & Part B)	GIS Application (For entire BharatNet Ph-1, 2,3 fiber route) - Qty 1	The requested Qty for GIS & related application as part of bid is 1. While uptime requested in non-functional requirements is 99.99%. This is contradictory, please clarify or correct it. 99.99% uptime is possible with 1+1 Active-Active Redundancy	-	Pls go through RFP. We are expecting high performance and high uptime application architecture with almost zero risk of blackout. The bidders are advice to understand and do proper due diligence at product level individuality and totality to meet overall functional, business objectivity and business continuity.
1097	164	Financial Bid Format (Part A & Part B)	Operational Visibility Platform (OVP) + OSS and BSS functionality	The requested Qty for OVP + OSS/BSS functionality as part of bid is 1. While uptime requested in non-functional requirements is 99.99%. This is contradictory, please clarify or correct it. 99.99% uptime is possible with 1+1 Active-Active Redundancy	-	Pls go through RFP. We are expecting high performance and high uptime application architecture with almost zero risk of blackout. The bidders are advice to understand and do proper due diligence at product level individuality and totality to meet overall functional, business objectivity and business continuity.
1098	49	4.2 Operational Visibility Platform (NMS + OSS + BSS+	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing .	By deploying the testing agents will help perform monitorng the the Network based KPIs like Packet loss,latency,jitter	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		Network visibility):2 Functional Requirement	two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	However to achieve the path tracing between GP to NOC and GP to Internet OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.		
1099	51	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):4 Network Topolozy and Visulaization	Network path visualization: a time-correlated, unified view of all paths between any two points on network. With visibility across network, application, routing, and device layers.	To get the network path visualization deploying light weight software/hardware based testing agents is allowed and ICMP/TTL propagation is enabled .	By deploying the testing agents will help monitor the Network path and get the visualizations of paths.	Pls refer preceding response
1100	52	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): 6 Network scanning	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing . However to achieve the path tracing between GP to NOC and GP to Internet	By deploying the testing agents will help perform monitorng the the Netwokr based KPIs like Packet loss,latency,jitter	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.		
1101	135	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 3	The proposed solution should support synthetic network test at both ends of a monitored path (GP to S-NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput–an improved form of the bandwidth metric–along with Path Visualization and path MTU.	By deploying custom software/hardware based testing agents at each GPs and NOC to perform tha path tracing . However to achieve the path tracing between GP to NOC and GP to Internet OR NOC to GP and NOC to Internet with ICMP/TTL propagation is enabled.	By deploying the testing agents will help perform monitorng the the Netwokr based KPIs like Packet loss,latency,jitter	Pls refer preceding response
1102	135	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 1	The Proposed solution should have an architecture supporting ease of deployment, zero touch maintenance and seamless monitoring could be on premise or MeitY empaneled cloud based.	The word should be rewritten as "The Proposed solution should have an architecture supporting ease of deployment, zero touch maintenance and seamless monitoring could be on premise or may	-	Repeated query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				be on empaneled/**secured** cloud based.		
1103	136	6.3 4S vision c) Service Performance Monitoring (Qualitative Service Visibility): 9	Real time visibility & monitoring of both Network and Application(s) for better co-relation of the Service impact pro-actively rather than re-actively. (Milli Second Level visibility: 20pps to 1000 pps for real time monitoring) for continuous real time KPIs and SLA reporting.	Pls modify this as follows " (Milli Second Level visibility: 10pps to 100 pps for Near real time monitoring)	If the traffic is sent with higher number of pps to target servers/link which might face some rejection from target servers which will affect the monitoring of services.	Repeat Query , already allowed
1104	136	23. Network Element Management System - > 24.> c) Service Performance Monitoring (Qualitative Service Visibility): 16	Additional Point	Solution shall support deploying lightweight, software-based agents to monitor key internal or cloud-based applications and services.	Testing methodology	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1105	136	23. Network Element Management System - > 24.> c) Service Performance Monitoring (Qualitative Service Visibility): 17	Additional Point	Solution shall provide easy sharing of interactive monitoring views to aid internal teams and external providers and vendors to collaborate to solve problems fast.	Keeping transperancy while sharing the data	Pls refer preceding response
1106	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 500GB SSD.	**Justification:** Network security solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance. Also, it is not recommended to have	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					built-in bypass as best practice.	
1107	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 3	Device should support at least 80Gbps throughput	Please suggest whether 80 Gbps mentioned is legitimate throughput or mitigation capability.	-	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1108	60	4.5 Link Load Balancer, Point no. 1 Features	Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.	**Hence requesting you to change this point as below:** Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 500GB SSD.	**Justification:** Network solutions should not store any logs on hardware appliance, as a best practice. These logs should always be stored at central repository location. This is to retrieve the logs in case of the hardware failure. Hence, requesting to remove the point to have 4 TB SSD in-built the appliance.	This is performance related ask. The request of downgrading anything by 1/8th seems downsize product. However, for slight variation and fitment of product, the general tolerence of 10% +/- is acceptable.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1109	61	4.5 Link Load Balancer, Point no. 2 Security	Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation	**Requesting you to Plesae remove this point.**	**Justification:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a stateful device. This is relevant for DDoS solution	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1110	62	4.5 Link Load Balancer, Point no. 2 Security	Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist –	**Requesting you to Plesae remove this point.**	**Justification:** Link Load Balancer is solely used for purpose of load balancing internet traffic for opimum use of internet links. To expect additional task of protecting DDoS aatacks is not recommended from LLB kind of solution. DDoS is always recommended to be **Stateless technology**, however LLB is a	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic		stateful device. This is relevant for DDoS solution	
1111	62	4.5 Link Load Balancer, Point no. 3 Global Load Balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one	**Requesting you to Plesae remove this point.**	**Justification:** Customer like GFGNL should have full-fledged dedicated solution for DNS and should not be part of ADC solution. Also we will recommend GFGNL to have DNS server on at centralised location to ensure high availability and smooth functioning of organisation and it should be a dedicated solution offering and should not be clubbed with ADC kind of solution. Every OEM has their own mechanism to manage Global load balancing functionality. Authoritative for Global load balancing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1112	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	**Justification:** DDoS technology has to be stateless so that it can handle an unlimited number of concurrent attack sessions. If the solution is stateful, it will have limits on the TCP session table for various attack types. The context emphasizes that any DDoS solution that is not stateless is susceptible to being a victim of a denial of service attack by exhausting resources and session table entries.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
1113	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Support for TLSv1.3 Perfect Forward Secrecy (PFS) Hardware Acceleration.	**Justification:** With TLSv1.3 coming into existence, the DDoS attack sophistication has moved to next level. Hence, it becomes necessary to have TLSv1.3 support to mitigate such attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1114	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The OEM must be presented in Leaders quadrant of latest IDC or Forrester or Sparks Matrix Report for DDoS.	**Justification:** Recognition by 3rd party analysts gives assurance of better DDoS solution and technology.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1115	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be capable to generate attacks signatures automatically within 15 seconds for zero-day attack protection.	**Justification:** To protect from any automated Zero-Day DDoS attack, it is of utmost important to mitigate such attacks. The DDoS solution should be capable enough to detect, characterize and generate optimal signatures to block such unknown attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1116	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed DDoS appliance must be able to handle unlimited attack concurrent session without any limitations and should be clearly mentioned in public facing datasheet	**Justification:** There should be no limitation when it comes to handle attack concurrent session by DDoS solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1117	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS appliance must be able to detect and block Zombie Floods	**Justification:** DDoS solution should have capability to detect and mitigate different types of	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					sophisticated flood attacks.	
1118	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The DDoS Appliance must be able to block invalid packets including checks for : Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped	**Justification:** DDoS solution should have capability to detect and mitigate different types of sophisticated flood attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1119	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The proposed solution should be standalone dedicated hardware appliance-based solution for DDoS Detection and Mitigation and NOT	**Justification:** The whole purpose of DDoS is it should be stateless device to handle volumetric and other sophiticated DDoS attacks. Being stateful device beats	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device, should not modify the MAC address of the packets or MAC or IP addresses of passed frames with all below features enabled and it should support Active - Active and Active - Passive deployment	the purpose of DDoS device as the device will fail once the session table fills up in case of TCP, UDP etc. flood attacks.	
1120	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Should support **latency less than 80 microseconds** and should be clearly mentioned in data sheet on public facing web portal.	**Justification:** Lesser latency is optimum for any organisation to improve user experience. The latency tends to increase during DDoS attack which can impact user productivity and business.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1121	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System includes a scalable SSL TPS capacity, either internally and should have option to integration of external appliance	**Justification:** DDoS solution should have capability to detect and mitigate encrypted flood attack using different techniques.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				for SSL TPS scalability		
1122	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	System should support following environments for mitigation of all kinds of traffic including but not limited to (UDP, TCP, DNS, HTTP, HTTPs) : a) Symmetric b) Asymmetric Ingress c) Asymmetric Mesh	Justification: DDoS solution should have capability to detect and mitigate different protocol attacks.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1123	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	The Proposed Solution should have capability to be deployed in Inline mode or Out-of-Path mode	**Justification:** For service provider kind of customer, it is recommended to have solution deployed out-of-path for reduced latency.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1124	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Proposed OEM should give highest level of support directly from OEM, such that customer can raise case with OEM directly	**Justification:** Support provided directly by OEM is highly recommended in case of any issues faced for better timely resolution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1125	-	4.4 DDoS - Distribute	Additional Clause	Proposed OEM should be deployed and used by at least	Proposed OEM should be deployed and used by at least 2 Tier-1	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		d Denial-of-Service		2 Tier-1 service providers for DDoS mitigation in India	service providers for DDoS mitigation in India	
1126	-	4.4 DDoS - Distributed Denial-of-Service	Additional Clause	Solution should be Make In India Class 1	**Justification:** India make solutions should be given preference. Make In India is Government of India scheme intended to boost the domestic manufacturing sector. Being a government entity, initiatives taken by Indian Government should be well encouraged.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1127	-	4.5 Link Load Balancer	Additional Clause	Resource reservation between each virtual load balancer instances with capability to run in Virtualized as well as Standalone mode. Such that these (Virtualized as well as Standalone) mode should be interchangeable via CLI and GUI with click of button (Bidder may be asked to demonstrate this feature during Technical Evaluation).	**Justification:** The solution should support specialized ADC hypervisor that runs multiple virtual ADC instances on dedicated ADC hardware. This specialized hypervisor should run fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. Application images are used by Virtual ADC and Standalone ADC. This virtualised mode should not have ability to run third party OS (This will make sure that KVM like Hypervisor not used on LB, and will remove possilbity of installing malacious OS)	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1128	81	System Memory	Min 768 GB DDR-5 or Latest, supported up to 4 TB or higher with 24 or more DIMM slots; ECC Advance	Kindly modify the clause as "Min 768 GB DDR-5 or Latest, supported up to 4 TB or higher with 24 or more DIMM slots; ECC"	Kindly modify for wider participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1129	81	Server Interface	Serial Port, 2 x USB 3.2 Gen 1Port,	kindly modify the clause as "-Serial Port, 2 x USB 3.0/3.2 Gen 1 Port,"	Kindly modify for wider participation as both have same transfer speeds.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1130	82	System Security	Secure erase of NAND/User data	Kindly modify as "Secure Erase"	Kindly modify the clause as its OEM specific	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1131	-	Server Security Features-2	Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.	Kindly ammend it as "" Solution should support firmware rollback	The current clause is OEM specific. Every OEM have different architecture for firmware rollback. Kindly amend the clause to qualify and wider participation."	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1132	89	Backup Server Interface	2 x USB 3.2 Gen1 ports or higher	kindly modify the clause as " 2 x USB 3.0/3.2 Gen 1 Port or higher,"	Kindly modify for wider participation as both have same transfer speeds.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1133	90	Backup server System Security	Secure erase of NAND/User data	Kindly modify as "Secure Erase"	Kindly modify the clause as its OEM specific	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1134	90	Backup Firmware security	Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	Kindly ammend it as "Solution should support firmware rollback"	The current clause is OEM specific. Every OEM have different architecture for firmware rollback. Kindly amend the clause to qualify and wider participation."	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1135	91	Backup server Embedded Remote Management and firmware security	Server should support storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware.	Kindly ammend it as " Solution should have remote management to manage repository for firmware, drivers, and software components "	The current clause is OEM specific. Every OEM have different architecture for remote management. Kindly amend the clause to qualify and wider participation.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1136	91	Backup server Embedded Remote Management and firmware security	Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation.	Kindly modify the clause as "Remote console sharing up to 2 users simultaneously during pre-OS and OS runtime operation."	Current clause is OEM specific, For wider participation, kindly modify the clause.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1137	57	4.3 Network Intrusion Prevention System (NIPS) / 2	• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency	• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 140Gbps on the same box (1 RU) supporting 60M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL.	The organization's network size and growth rate do not necessitate stacking to achieve 400 Gbps. Also a single appliance can handle the network's throughput requirements upto 140Gbps. The latency parameter can change based on multiple parameters like type of port , bandwidth , security configurations in the solution , load on the solution etc. therefore necessiate the changes.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1138	58	4.3 Network Intrusion Prevention System (NIPS) / 3	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure.	Should be an on-premise standalone NIPS appliance.	Please consider the changes as this blocks many security vendors like us to participate .	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1139	63	4.6 Next Generation Firewall /2	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active, Active/Passive and HA clustering support.	The firewall should have minimum 4 x100/40G,4x10G/25G and 4 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active (HA clustering support) and Active/Passive.	The changed interface density will suffice the requirement. It will not affect the overall ask.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1140	63/64	4.6 Next Generation Firewall /2	• The Appliance must handle the threat prevention throughput of minimum 60 Gbps enabling security features and measured with Enterprise Mix /Application Mix traffic. • The Firewall must deliver minimum 80 Gbps of IPSEC throughput from day 1.	• The Appliance must handle the threat prevention throughput of minimum 100 Gbps scalable upto 140 Gbps enabling security features and measured with Enterprise Mix /Application Mix	The threat prevention throughput asked is quite low with respect to the concurent session asked, hence increasing it. Also reducing the new connection per second to 800K with AVC enable The throughput	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			• The Appliance should support minimum New Connections per Sec of 1 million. • The Application should have Concurrent Sessions of – 60 million from day one.	traffic. • The Firewall must deliver minimum 80 Gbps of IPSEC throughput from day 1. • The Appliance should support minimum New Connections per Sec of 800K with AVC. • The Application should have Concurrent Sessions of – 60 million from day one.	will also go in sync with NIP's.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1141	64	4.6 Next Generation Firewall / 5	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window can be schedule or automatic** **• Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV action such as allow, deny/drop,alert etc.** **• NGFW should have**	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware/IPS signatures and should have minimum signatures update**	CDR is a functionality of email security solution and this can be achieved using email security in conjunction of NGFW which are specialized for content sanitization. This is not a primary focus of firewall. SSH inspection causes SSH traffic , breaks the connection and causes issues in regaining connection.There is no specific use case of SSH inspection. These are all specific to OEM, kindly update the changes for better particiation and with the changes suggested the functional requirement remains same.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time. **• IPS must deliver more than 10000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect against Denial of Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces	**window can be schedule or automatic** **• Should be able to perform Anti-virus /IPS scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV/IPS action such as disable, deny/drop,alert etc.** **• NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time.** **• IPS must deliver more than 20000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			policies with various categories and ability to queries a real time OEM threat intel database • **The NGFW should have both SSL and SSH Inspection capabilities"**	against Denial of Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies with various categories and ability to queries a real time OEM threat intel database • **The NGFW should have both SSL or SSH Inspection capabilities"**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1142	76	**4.12 AAA Server/ 5**	AAA Solution should be scalable enough to support added endpoints in the network. Facility to integrate with multiple devices and gateways i.e SMS, Payment, Email ..etc.	AAA Solution should be scalable enough to support added endpoints in the network. Facility to integrate with multiple devices and gateways i.e SMS, Email ..etc.	For a NAC, there won't be a use case for payment as a gateway. Please remove the same.	The AAA (Authentication, Authorization, and Accounting) server is required to authenticate NOC users securely, ensuring controlled access based on predefined roles and policies. The solution must support integration with multiple authentication methods, including LDAP, RADIUS, TACACS+, and multi-factor authentication (MFA), to enhance security. Additionally, audit logs should be maintained for compliance and monitoring purposes.
1143	182	9.2 Annexure A Part 2 - Scope of Work as per BharatNet ABP RFP	1. GIS data collection • PIA of GFGNL ABP RFP shall conduct survey of the Block and associated routes from Block to Gram Panchayats (GPs) to evaluate the existing and new fiber cable needs for network implementation.	We understand that the PIA of RFP Ref No: GFGNL/GFG/e-file/263/2025/0016 /NOC is not responsider for any field related survey & data collection. Please confirm	To derive the exact scope under the RFP	Understanding is correct
1144	73	4.9 Core Router:	Functionality : The router shall be TEC-GR: TEC 48050:2024	We understand router should only comply with TEC 48050:2024 clouses , cirtification not required for same.	To derive the exact scope under the RFP	Need to comply Latest Tech GR
1145	74	4.10 Core Switch:	Interface and Performance TEC GR 480060:2023	We understand Core Switch should only comply with TEC GR 480060:2023 clouses , cirtification not required for same.	To derive the exact scope under the RFP	As per clarification sought

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1146	23	2.1 Introduction Objective of Phase III:	VII. Socio-Economic Empowerment: Facilitate digital empowerment by enabling access to education, healthcare, e-governance, and economic opportunities in rural areas. Deployment of mini-OLT at every two GPs with target of approx. 6 lakhs customer over BharatNet network.	We understand that these 6 lack subscriber provisioning & OLT configuration is not part of GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016 /NOC RFP scope.	Need to factor the service provisioning cost	Provisioning is to be done by the PIA of PH-III RFP however, to fulfill the task software, storage and customization are to be facilitated by the SI of this RFP
1147	26	3.1.1 Eligibility Criteria: Serial no :- 2	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	Request GFGNL to amend the clause as below "The bidder should have average turnover of minimum INR 100 crores from ICT/IT/ITeS system integration in any three financials years of the last seven financial year as on 31st March 2024:"	ICT/IT/ITeS system integration is more align with the nature of work under this RFP.	Pls see revision
1148	27	3.1.1 Eligibility Criteria: Serial no :- 4	Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage,	We understand that Implementation, Operation & Maintenance of command control center would also be considered	Both Command Control Center & NOC are similar type of project.	As per the RFP SoW the ask is to monitor the PH-III implementation and operation and maintain ace of the same. Pls also refer the 4S vision for further clarity

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Security and Networking components) and managing, monitoring network nodes as a part of the Project	under similar project.		
1149	27	3.1.1 Eligibility Criteria: Serial no :- 4	Copies of Purchase Order, completion/ Go live certificate or partial completion certificate complying to the clause requirement from client to be enclosed along with Technical Bid.	We understand that incase of consortium bids submitted in other project ,lead bidder of that project can clainm the entire experiance.	As per industry practice	Understanding is correct
1150	29	3.1.1 Eligibility Criteria: Serial no :- 9	The Bidder must possess any three of the following certifications as on date of bid submission - a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	Request GFGNL to replace below clause against b) ISO/IEC 20000-1:2018…. To be replace with b) ISO /IEC 140001:2015	As per industry practice	As per RFP
1151	36	4.1 Geographical Information System (GIS): Serial no :- 2	2. PM Tool	We understand that the PIA of RFP Ref No: GFGNL/GFG/e-file/263/2025/0016 /NOC is to produce the dashboard only the input data to be updated by GFGNL.	Clarity will help to understand the scope to arrive the cost.	As per RFP
1152	37	4.1 Geographical Information System	API Integration Enable integration with SMS, email, and WhatsApp gateways for	We understand that PIA of RFP Ref No: GFGNL/GFG/e-file/263/2025/0016 /NOC is to only	Clarity will help to understand the scope to arrive the cost.	Pls refer preceding response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		(GIS): Serial no :- 3	communication with field technicians/customers	enable the system for Integration with SMS , email & whattsapp. The SMS,email & whatssapp gatwar charges will be borned by GFGNL seperately.		
1153	42	Serial no 14 Fiber Inventory Mobile App	Include voice-based network creation features for point objects (e.g., “Create an OLT” command).	Request to remove this clause as this is a single vendor feature or allow Voice-based / Manual way of Network creation	this will limit the multiple GIS OEM to participate	Pls see revision
1154	133	6.3 4S vision	b) Service provisioning (Automated):	We understand that under this RFP there is no Subsriber provisioning is involved. Only Network / Router / Transport equipment provioining & mainteance is involved.	To derive the exact scope under the RFP	Pls go through RFP and 4S section. However for your reference it is to be explained that the boundary of subscriber is Gov. public institutions, Enterprise partners and villages. Broadly individual households is out of scope.
1155	133	6.3 4S vision	b) Service provisioning (Automated):	Request to please share the maximum number of Subscriber & type of Subscriber provisioning is requied.	To derive the exact scope under the RFP	Pls go through RFP and 4S section. However for your reference it is to be explained that the boundary of subscriber is Gov. public institutions, Enterprise partners and villages. Broadly individual households is out of scope.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1156	170	9.1 Annexure A Part 1 - Technical Specification for GIS Mapping of OFC Routes	2) Accuracy: Meter level accuracy (20 CM)	We uderstand that all field related activity such as Survey, Measurement book & As built diagram is not part of this RFP	To derive the exact scope under the RFP	Understanding is correct
1157	170	9.1 Annexure A Part 1 - Technical Specification for GIS Mapping of OFC Routes	2) Accuracy: Meter level accuracy (20 CM)	We understand that the equipment required to get 20 CM accuray is resposibility of GFGNL	To derive the exact scope under the RFP	Understanding is correct
1158	170	9.1 Annexure A Part 1 - Technical Specification for GIS Mapping of OFC Routes	2) Accuracy: Meter level accuracy (20 CM) 3) 50% collection of Lat/Long should be up to 1 Meters accuracy 4) 95% collection of Lat/Long should be up to 2 Meters accuracy.	Request more details why 3 separate accuracy has been asked.	To derive the exact scope under the RFP	Pls see revision
1159	170	9.1 Annexure A Part 1 - Technical Specification for GIS Mapping	6) Base Map for Validation: NIC Base map.	We understand that NIC Base map will be arranged by GFGNL.	To derive the exact scope under the RFP	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		of OFC Routes				
1160	Page 26	3.1.1 Eligibility Criteria **Point-2**	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	**"We kindly request the removal of this clause for bidder participation." CLRA** The bidder should have average annual turnover of minimum INR 100 Crores from **IT/ICT** ~~ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration~~ in any three financial years out of last four Financial Year as on 31st March 2024.	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1161	Page 27	3.1.1 Eligibility Criteria **Point-4**	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: **a) One project with the value of at least 40 crores with 5K network Nodes or** **b) Two projects, each with the value of at least 30 crores with 4K network Nodes or** **c) Three projects, each with the value of at least 20 crores with 3K network Nodes** Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	**"We kindly request the removal of this clause for bidder participation."** The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: **a) One project with the value of at least 40 crores ~~with 5K network Nodes or~~** **b) Two projects, each with the value of at least 30 crores ~~with 4K network Nodes or~~** **c) Three projects, each with the value of at least 20 crores ~~with 3K network Nodes~~** Similar Project is defined as:	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.		
1162	Page 30	3.2.1 Technical qualificati on criteria **Point 1**	The bidder should have supplied, implemented and managed following projects in past 5 years. **a)** NOC (Network Operation Center)- **3 Marks** **b)** Data center- **3 Marks** **c)** NOC, Data center, (NMS/OSS or Network GIS)- **9 Marks** **Note:** • The highest experience based will be given highest marks and there after rest will be given marks on percentile basis.	**We kindly request that this clause be modified to allow for bidder participation."** The bidder should have supplied, implemented and managed following projects in past 5 years. **a)** ICCC (Integrated Cammand cantrola Center)- **3 Marks** **b)** Data center- **3 Marks** **c)** ~~NOC~~, Data center, (NMS/OSS or Network GIS)- **9 Marks**	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Note: • The highest experience based will be given highest marks and there after rest will be given marks on percentile basis.		
1163	Page 31	3.2.1 Technical qualificati on criteria **Point 4**	Visualization/orchestration in setting up and management for S-NOC (Private -on premise Cloud)	**We kindly request that this clause be modified to allow for bidder participation."** Visualization/orches tration in setting up and management for ~~S-NOC (Private - on premise Cloud)~~ Data Center/ ICCC (Integrated Cammand cantrola Center)	-	Pls see previous response
1164	-	-	-	We could not find any clarity on Consortium, if consortium is not permitted, then we would request the Authority to **kindly allow to form a Consortium.**	Looking to the type of solutions / deliverables (Networking, Security, GIS, OSS, BSS, NMS, Storage, back-up etc.), the importance of the project, consortium will strengthen the overall technical capabilities & richness in the	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					experience, this would result in better, faster & optimized deployment of solution and services.	
1165	25	3.1.1 Eligibility Criteria Point # 2	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	We request Authority to kindly amend the said clause as, "The bidder should have average annual turnover of minimum INR 100 Crores ***from IT / ICT System Deployment*** in any three financial years out of last four Financial Year as on 31st March 2024.	The overall scope of work is comprising of supply / deployment of IT components (Server, Storage, Backup, Router, Switches, NGFW, NIPS, DDoS, Applications such as GIS, OSS, BSS, Mobile apps, NMS etc. and providing Onsite set of Manpower (minimum 14 nos.) for O&M.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1166	27	3.1.1 Eligibility Criteria Point # 4	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India **during past five year**s from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	1) We request authority to kindly expand the experience window of within 5 years **to 8 years (either the project tenure should have completed OR can be Ongoing, if Go-live is acheived**. 2) We request the Authority to amend the defination of Similar Projects as, ***"Similar Project is defined as: Supply / deployment of IT Infrastructure that is compute, storage, Security, Networking components etc. at Network Operation Centre or State NOC or Data Centre."***	Requested defination gives better clarity that the Scope of Work is limited to supply, implemantation and O&M support for the IT equipments/ applications at NOC or SNoC or DC and similar projects would qualify.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1167	119	Pg No. 119, CAMC (Comprehensive Annual Maintenance Contract)	CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value	request to remove this point; Please add Capex to Opex Ratio should be 80% : 20%.	All OEM will bill material and 7 years services from Day 1 as per GFGNL ask; So if 7% CAMC PA asked bidder need to load heavy Cost of Finance on Capex and bid will jack up abruptly.	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.
1168	29	Pg. No. 29 BID EVALUATION PROCESS	The evaluation will be based on QCBS (30:70) i.e., 30% weightage will be given to technical score and 70% weightage will be given to financial.	The evaluation will be based on QCBS (70:30) i.e., 70% weightage will be given to technical score and 30% weightage will be given to financial.	This is very Critical Scope of work in terms of Technology; GFGNL DWDM bid with 70:30 & Phase 3 with 50:50 QCBS. As NoC bid required technical skills on multiple factors; Please consider 70:30 QCBS.	Pls see revision
1169	126	Pg. No. 1226, 6.1.14 : AMC of Old Devices	Bidder shall take the HOTO of existing IT infra like Video wall, computer terminals and Non IT infra like furniture, UPS. AMC of the these infra shall be responsibility of the bidder. Information is given in Annexure B.	Please ask for New UPS and Videowall for this RFP.	The UPS & Videowall is already crossed his Life and the cost to maintain this for next 7 to 10 Years is not practical; So please ask for latest product and allow buy back of this assets to bidder.	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
1170	58	4.4 DDoS - Distributed Denial-of-Service	(2) Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	Different OEMs have different ways to fulfil the solution requirement. Requesting 4 TB SSD may limit the participation.	Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual power supply & memory as per solution requirement.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Kindly allow bidder to provide memory as per solution requirement.		
1171	72	4.9 Core Router	Core Router, BNG, Carrier Grade NAT, DDoS	Different OEMs have different ways to fulfil the solution requirement. Kindly allow the bidders to quote single or multi-box solutions to achieve the functionalities of Core Router, BNG, Carrier Grade NAT, DDoS for wider participation.	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, DDoS as per RFP.	GFGNL intends to connect all the Gram panchayats in the state of Gujarat. Broadband connectivity across the state of Gujarat would be in very large numbers, considering the scale GFGNL has decided to have separate infrastructure for each of the functions asked. However for wider participation bidder can quote multiple network hardware for different functionalities asked in RFP.
1172	69	4.8 Carrier Grade NAT	(1) Hardware Architecture •The appliance-based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one	CGNAT, AVC, IPS are different functionalities. Every OEM have different ways to meet the solution requirement. Kindly allow bidder to quote single or multibox solution for wider participation.	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, AVC, IPS, DDoS as per RFP.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1173	66	4.7 BNG	(1) General Capabilities The solution should have external NAT capability	This clause is very restrictive in nature as it mandates the NAT capability outside of BNG.	The solution should have NAT capability achieved through same box or multi-box solution.	GFGNL intends to connect all the Gram panchayats in the state of Gujarat. Broadband connectivity across the state of Gujarat would be in very large numbers, considering the scale GFGNL has decided to have separate infrastructure for each of the functions asked. However for wider participation bidder can quote multiple network hardware for different functionalities asked in RFP.
1174	66	4.7 BNG	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps switching capacity with 2200 Mpps forwarding performance.	Mentioning throughput in Mpps is very specific to and favoring particular OEM, kindly mention throughput requirment in Tbps for wider participation.	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps FD switching capacity. All the necessary hardware, software and licenses must be supplied with the chassis from day-1 with life-time validity of licenses.	Removing specific ask for wider participation. The user plane / data plane solution should have minimum 8 Tbps switching capacity with adequate forwarding performance to meet traffic requirements. The objective is wider participation and for such minor level numeric will not be reason for disallowing products.
1175	69	4.8 Carrier Grade NAT	(5) Management Functions	This architecture is specific to OEM and restricts participation.	Bidder is allowed to meet the technical requirement of management through EMS.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1176	72	4.9 Core Router	(7) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1177	72	4.9 Core Router	(4) Routing and protocols Segment routing, SR TE, SR PCE, SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	For wider participation	Segment routing, SR TE, SR PCE / SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1178	74	4.10 Core Switch	(1) Architecture The switch should be a chassis based switch and should have at least 6 payload slots.	This clause is very restrictive in nature as the bidder must be allowed to quote as many slots required to meet the technical requirement of solution. Requesting 6 slots in particular is restricting wider participation.	The switch should be a chassis based switch and should have multiple payload slots. Interfaces mentioned in the RFP must be populated on the field-removable line-card payload slots only. Any interfaces provided on-board on chassis or controller cards should not be considered in response to the required solution.	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
1179	74	4.10 Core Switch	(1) Architecture It shall support 1:1/N+1 redundancy and reliability for critical features such as components power supplies and fans to eliminate single points of failure.	Since modular switch is requested with payload slots for future expansion, the most important and critical reliability aspect of having redundant controller card must be considered. Requesting for high throughput modular chassis without redundant	It shall support 1:1/N+1 redundancy and reliability for critical features such as controller cards, power supplies and fans to eliminate single points of failure	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				controller card will put critical traffic at stake.		
1180	74	4.10 Core Switch	(2) Interface and Performance The Switch should have a minimum 2.4Tbps of non-blocking performance. The switch shall support minimum 24 x40/100G on day 1 and also support additional line cards for future expansion.	Requesting 2.4 Tb throughput with Day-1 interface requirement of 24 x 100G = 2.4 Tb already consumes the entire throughput of chassis and then requesting for multiple payload slots for future expansion defeats the purpose of having the slots. Requesting you to dimension future throughput requirement in the chassis performance to avoid bottle-necks in future.	The Switch should have a minimum 4 Tbps FD of non-blocking performance. All the necessary hardware, software and licenses must be supplied with the chassis from day-1 with life-time validity of licenses.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
1181	74	4.10 Core Switch	(4) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				temperature clause for 5 to 40 degree C		
1182	75	4.11 Access Switch	(4) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. The additional functionalities stands optional for unnecessary eliminations.
1183	58	4.4 DDoS - Distributed Denial-of-Service	(2) Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	Different OEMs have different ways to fulfil the solution requirement. Requesting 4 TB SSD may limit the participation. Kindly allow bidder to provide memory as per solution requirement.	Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual power supply & memory as per solution requirement.	This is performance related ask. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the purpose is link load balancing. The additional functionalities stands optional for unnecessary eliminations.
1184	72	4.9 Core Router	Core Router, BNG, Carrier Grade NAT, DDoS	Different OEMs have different ways to fulfil the solution requirement. Kindly allow the bidders to quote single or multi-box solutions to achieve the functionalities of Core Router, BNG,	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, DDoS as per RFP.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Carrier Grade NAT, DDoS for wider participation.		
1185	69	4.8 Carrier Grade NAT	(1) Hardware Architecture •The appliance-based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one	CGNAT, AVC, IPS are different functionalities. Every OEM have different ways to meet the solution requirement. Kindly allow bidder to quote single or multibox solution for wider participation.	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, AVC, IPS, DDoS as per RFP.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1186	66	4.7 BNG	(1) General Capabilities The solution should have external NAT capability	This clause is very restrictive in nature as it mandates the NAT capability outside of BNG.	The solution should have NAT capability achieved through same box or multi-box solution.	GFGNL intends to connect all the Gram panchayats in the state of Gujarat. Broadband connectivity across the state of Gujarat would be in very large numbers, considering the scale GFGNL has decided to have separate infrastructure for each of the functions asked. However for wider participation bidder can quote multiple network hardware for different functionalities asked in RFP.
1187	66	4.7 BNG	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps switching capacity with 2200 Mpps forwarding performance.	Mentioning throughput in Mpps is very specific to and favoring particular OEM, kindly mention throughput requirment in Tbps for wider participation.	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps FD switching capacity. All the necessary hardware, software and licenses must be supplied with the chassis from day-1 with	Removing specific ask for wider participation. The user plane / data plane solution should have minimum 8 Tbps switching capacity with adequate forwarding performance to meet traffic requirements. The objective is wider participation and for such minor level numeric will not be reason for disallowing products.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					life-time validity of licenses.	
1188	69	4.8 Carrier Grade NAT	(5) Management Functions	This architecture is specific to OEM and restricts participation.	Bidder is allowed to meet the technical requirement of management through EMS.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1189	72	4.9 Core Router	(7) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. The additional functionalities stands optional for unnecessary eliminations.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1190	72	4.9 Core Router	(4) Routing and protocols Segment routing, SR TE, SR PCE, SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	For wider participation	Segment routing, SR TE, SR PCE / SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
1191	74	4.10 Core Switch	(1) Architecture The switch should be a chassis based switch and should have at least 6 payload slots.	This clause is very restrictive in nature as the bidder must be allowed to quote as many slots required to meet the technical requirement of solution. Requesting 6 slots in particular is restricting wider participation.	The switch should be a chassis based switch and should have multiple payload slots. Interfaces mentioned in the RFP must be populated on the field-removable line-card payload slots only. Any interfaces provided on-board on chassis or controller cards should not be considered in response to the required solution.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1192	74	4.10 Core Switch	(1) Architecture It shall support 1:1/N+1 redundancy and reliability for critical features such as components power supplies and fans to eliminate single points of failure.	Since modular switch is requested with payload slots for future expansion, the most important and critical reliability aspect of having redundant controller card must be considered. Requesting for high throughput modular chassis without redundant controller card will put critical traffic at stake.	It shall support 1:1/N+1 redundancy and reliability for critical features such as controller cards, power supplies and fans to eliminate single points of failure	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1193	74	4.10 Core Switch	(2) Interface and Performance The Switch should have a minimum 2.4Tbps of non-blocking performance. The switch shall support minimum 24 x40/100G on day 1 and also support additional line cards for future expansion.	Requesting 2.4 Tb throughput with Day-1 interface requirement of 24 x 100G = 2.4 Tb already consumes the entire throughput of chassis and then requesting for multiple payload slots for future expansion defeats the purpose of having the slots. Requesting you to dimension future	The Switch should have a minimum 4 Tbps FD of non-blocking performance. All the necessary hardware, software and licenses must be supplied with the chassis from day-1 with life-time validity of licenses.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				throughput requirement in the chassis performance to avoid bottle-necks in future.		
1194	74	4.10 Core Switch	(4) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.
1195	75	4.11 Access Switch	(4) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1196	112	Limitation of liability	Selected agency's cumulative liability for its obligations under the contract shall not exceed the value of the pending part of the assigned orders anytime by the TENDERER within the contract term on the day claim is raised	Selected agency's cumulative liability for its obligations under the contract shall not exceed value of the annual contract applicable for the day claim is raised. Selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.	All large infrastructure contracts have risk purchase and other penal clauses allowing tenderer to terminate the contract and award to another party at the expense of the selected agency. The penalty charges are capped at 20% of overall Capex/Opex in RFP; liability cap of "annual contract value" is higher than these caps hence suffcient enough to recover damages by tenderer if any. Discharge of liability cap on annual basis keep the balance sheets clean, without passing on risks to next year; and the cost of liability cap (risks/contigency) lower thus helping bid to be more economical. Higher caps increase the value of risk and the bid values; which anyway are of no use for tenderer for all practical prupose.	Revised Clause for ease of doing business and disburden participants: Selected agency's cumulative liability for its obligations under the contract shall not exceed value of the annual contract applicable for the day claim is raised. Selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1197	112 and 113	5.27, 5.32	Whole clause of 5.27, 5.32 are not typed but relavant pt from clauses are pasted - 5.27 - Selected agency will defend and/or settle any claims against the TENDERER that allege that Bidder service and/or branded product as supplied under this contract infringes the intellectual property rights of a third party 5.32 - The Service Partner shall indemnify tenderer against all third-party claims of infringement of copyright, patent, trademark or industrial design rights arising from use of the Goods/services. In the event of any claim asserted by a third party, the Bidder shall act expeditiously to extinguish such claim	Request for deletion of 5.32	Section 5.27 is pragmatic but section 5.32 is exactly opposite and over protective. All OEMs give undertakings in the name of tenderer, they are also bidders (though not front ending) so are qually liable for their portion of solution and hence responsible for their acts of infringement in their quoted products. Selected agency has no means of verifying infrigments, other than digging history of the quoted products or OEMs. Selected agency can facilitate and support the tenderer for claming damages due to infringement	The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1198	119	Bullet 3 under Note	Aforesaid penalty cap will not be applicable for any severe impact/incident/outage at GSDC, resulting in loss to Government of Gujarat.	Request for deletion	This is very open ended as GSDC going down due to GFGNL infrastrcture is the issue at GSDC end. The placement of devices of GFGNL in GSDC will be following GSDC design guidelines so GSDC need to ensure that whole infra doesn't go down due to impact from GFGNL devices; that should be the level of agility in their solution. Also, there is no control of selected agency on GSDC infra, design or services to avoid such issue hence can't be penalized	GSDC outage is out of the scope.
1199	119	Bullet 2 under Note	CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value	70% of project payment are done till go-live and 30% over 7 years against CAMC. Then CAMC to be at least 7% of CAPEX; is the manpower cost separate from the 7% calculation?	Paying 70% of overall project value against go-live leave 30% for balance period, including manpower (project value = capex + CAMC + manpower) and the CAMC has to be 49% of CAPEX.. So whole maths doesn't workout. Either keep Manpower separate from project value	The requirement clearly states that the all OEM must provide a 7-year comprehensive warranty, and the bidder must ensure an extendable 3-year warranty, making a total of 10 years.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					(nothing else changes) OR change the %ges	
1200	119	Bullet 4 under Note	In case of any fault arises in the installed items during the warranty period of five years, bidder is requiring to either repair the faulty items or have to install the replacement (complying to the RFP specification) for faulty material without any additional cost to the Tenderer	In case of any fault arises repeatdely, for 3 times in the year, in the installed items during the warranty period of seven years, bidder is requiring to repair the faulty items or have to install the replacement (complying to the RFP specification) for such failure exceeding 3 times in a year) without any additional cost to the Tenderer	Replacement is essential when there are chronic issues or material defect or against repeated failures of same type	Pls see revision: • Defect period is 6 months. If any fault arises during the defect period it means it faulty product and therefore to avoid future recurrence it is mandatory to replace the item. • In case of any fault arises in the installed items during the warranty period of seven years, bidder is requiring to repair the faulty items. If, during the warranty period, any equipment has any failure on three or more occasions, due to hardware fault It shall be replaced by new equipment by the successful bidder at no cost to the GFGNL within 7 days.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1201	159	Pt 3,4 under sec 7.9	The penalty cap limit for CAPEX will be maximum to 20% of overall amount discovered in financial table for overall capex amount. And same will be applicable to 20% of overall amount discovered in financial table for overall OPEX amount The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 20% of Total Quarterly Payable	We understand that quarterly payment includes Operations & maintenance and manpower both; and all penalties put together should not exceed 20% of quarterly payment. Is the assumption right? 20% penalty is a higher number for service levels, we suggest to reduce to 10%	Since there is no separate pricing for OPEX (other than 30% to be paid over 7 years) and there is separate manpower charges asked in financial format; and also quarterly payment is not defined anywhere hence the query Also in 7.3 d (i) penalty exceeding 10% of quarterly payment for 2 consecutive quarters allowing tenderer to take action including termination; so both 7.3 d (i) should be in sync with Pt 4 under section 7.9	Repeated Query
1202	153	7.5, * Note under project timelines	T = Date of Award of GEM Contract/LoI.	T = Contract signing	GEM contract not applicable in this case Timelines for such critical project should start from contract signing not LOI (there is no BG at the time of LOI and only contract/work order is guarantee of the project)	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1203	153	7.5, Project timelines	All timelines are taken from T; does this mean penalty for not meeting milestone 2 (within 3 weeks); will be in addition to penalty for missing milestone 3 because if milestone is delayed than most likely further milestones may also delay. All penalties are on overall capex; is double whammy - first it is deducted on overall capex then even for delay occuring from previous milestone.	One of two should be corrected - either timetable resets from each milestone e.g. submission of PBG - T1 = T + 2 weeks; milestone 2 - T2 = T1 + 3 weeks… OR The penalty should be applied on milestone value NOT capex	These are the only ways to be reasonable with the application of penalty because if for some reason, one milestone gets delayed then bidder keeps paying penalty despite doing further milestones in expected "weeks to deliver" e.g. if bidder takes T+5 weeks in M2 and T+7 weeks in completing M3 then he pays penalty for both M2 and M3 despite doing justice for M3 (completing in 2 weeks as asked); ideally should be penalized for M2 only	Duplication of Penalty shall not be levied. The net days apportioned for particular milestone shall be considered expected days to finish that milestone. Any excess days beyond the net days shall be the portion of days for purpose of calculating the delayed days.
1204	154	7.6, penalties during O&M	1. Service availability - 0.01% of contract value per hour of system unavailability exceeding the Threshold.	Should be 0.01% of quarterly value per hour of system unavailability exceeding the Threshold.	Penalty on contract value is very harsh, should be on the applicable payments i.e. quarterly payments during OPEX and should be appliacble only when whole GFGNL NOC is down	Pls see revision for ease of business and disburden. Revised Clause: 0.01% of quarterly value per hour of system unavailability exceeding the Threshold.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1205	155	7.6, penalties during O&M	3. Security and data protection	Penalty on contract value for not fixing vulnerability and re-occurrence of vulnerability for which fixes were appliaed are way higher. Penalty should be on quarterly payment and re-occurrence penalty should be removed	The vulnerabilities are fixed as per the guidance given by OEMs or Cert-In; if those vulnerabilites reappear even after applying fixes then it can't be attributed to selected agency. If the fixes were not applied then anyway agency is getting penalized Also penalty should be on the relavant payments i.e. quarterly payment	Pls see revision. Penalty on quarterly payment.
1206	155	7.6, penalties during O&M	4. Data backup and recovery	Penalty on contract value for not taking backup is way higher. Penalty should be on quarterly payment and should increase with each incidence - 1. One such failure in quarter - 0.5% of QP 2. Two such failures in quarter - 2% of QP 3. Three such failures in quarter - 5% of QP	First time can be technical reason for failure but it is epxected from operations team to be better alerted next time hence failing again should be penalized more	Pls see revision. Penalty on quarterly payment.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1207	155	7.6, penalties during O&M	5. Support & escalation - exceeding 24hrs…	This is very subjective, whenever the period of resolution increases the escalations are bound to happen. These period vary for S1,S2 and S3 incidents. And all resolutions have escalation embeded in it. So, such penalty should be removed for no relavance	If time to resolve is increasing then anyway penalty is increasing for each window given for S1 (1hr), S2 (4hr), S3 (24hr) incidents then having one more penalty on escalation doesn't add any relavance. Already the matters would have been escalated for breaching these levels and agency will try everything to save from penalty. Also agency fears the contract termination for breaching maximum levels for 2 consecutive quarters	Since its already described in Sr No 2 incident Resolution with three types of priorities, if time exceed above 24 hours this penalty shall be levied.
1208	155	7.7 SLAs for patch managem ent	There are various slabs given for penalty for not meeting 4 categories of patch management (Critical, high….).	There are penalties on missing fixes on vulnerabilites in 7.6; then this section will create conflict. Either of these 7.6 (Pt 3) or 7.7 should be kept	Other than chosing one of two penalties 7.6/7.7 for patches; the penalty should be waived off for delay in fixing patches for those where systems may get impacted or patches are not getting right feedback from global communities or where tenderer approval is required.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1209	157	7.8 SLAs for change management	Delay in implementation of changes against agreed timelines for each change request - 2% of the total Quarterly billing amount for each week of delay	Penalty for not implementing request for critical change (impact is on overall system)- 1% of QP for each week of delay Penalty for not implementing request for important change (impact is on one sub-system) - 0.5% of QP for each week of delay Penalty for not implementing request for ordinary change (impact is on one technology/equipment) - 0.25% of QP for each week of delay	Request to keep different penalty for different change because all changes are not critical and also its evident from the delay window of 1 week kept in clause. If change was so critical that it gets penalty of 2% of QP then window should have been shorter or penalty should have been lower for 1 week of window Hence suggested slabs	Pls see revision.
1210	142	6.6 Manpower requirement	Bidder has to ensure availability of the manpower 24*7 in the NOC to provide network, software, security and related support to GFGNL, BharatNet Phase 3 PIA	Bidder has to ensure availability of the manpower for 24*7 support in the NOC for network, software, security and related support to GFGNL, BharatNet Phase 3 PIA. The necessary	14 resources are required as per table, then availability of 24x7 makes it 3 times of all resources as shifts are not specifically asked for any category of resource Better is to ask for staff	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				window for all resources to be available in NOC is "working hours"	to be available during working hours and on demand, to meet resolution/uptime SALs, for rest of the hours in 24hr day	
1211	158	7.10, 7.11	Software penalty, system outage, bug fixes etc.	The additional penalties mentioned in these sections create conflict with 7.6 and 7.7 hence duplication should be avoided (deleted)	All the penalties described in sections above are valid for both hardware ot software, most of the patches are applied on software only. When a patch is not applied on system then penalty is imposed as per table in 7.7, which is common to both hardware/software system. So there will be practical challenge in penalty imposition if these sections continue to remain valid in RFP.	Pls see revision.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1212	26	3.1.1 Eligibility Criteria:	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31 st March 2024.	We request you to please modify the clause: The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration **or Telecom or IT/ITES** in any three financial years out of last four Financial Year as on 31 st March 2024.	Justification: The proposed modification broadens the scope of eligible bidders by including revenue from Telecom and IT/ITES sectors. Given that Telecom and IT/ITES involve ICT system deployment, network operations, software product deployment, and integration services, they align with the core technical competencies required for this project. This change will ensure greater competition and allow experienced bidders from related industries to participate, thereby increasing the quality and competitiveness of the bids received.	For wider participation- Telecom or IT/ITeS is also allowed

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1213	26	3.1.1 Eligibility Criteria:	-	We kindly request you to permit the bidder to participate either individually or as part of a consortium. The Bidder may be a single entity or a group of at maximum of 3 (Three) entities (the "Consortium"), coming together to implement the project.	Allowing bidders to participate as a consortium provides the following benefits: **1. Enhanced Capabilities:** A consortium allows multiple entities to bring in their specialized expertise, ensuring better execution and innovation. **2. Increased Competition:** Encouraging consortium participation widens the pool of qualified bidders, leading to more competitive pricing and solutions. **3. Risk Mitigation**: Distributing responsibilities among multiple consortium members reduces the risk of project delays or failures. **4. Industry Best Practices:** Many large-	Consortium is not allowed

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					scale and complex projects require diverse skill sets, which can be better addressed by a consortium rather than a single entity.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1214	26	3.1.1 Eligibility Criteria:	-	We request addition of this clause : A bid submitted by a Bidder who has acquired a Company/ Division of a company/100% owned subsidiary company shall also be considered for evaluation if the eligibility and technical evaluation criteria are met jointly by the bidder and the Company/ Division acquired/100% owned subsidiary company.	Justification for the Requested Clause Addition: **Recognition of Business Acquisitions & Continuity**: Companies often acquire other entities or divisions to enhance their capabilities. Allowing such bidders to qualify ensures that expertise, resources, and past experience of the acquired entity are not disregarded. **Fair Evaluation of Capabilities:** If the bidder and the acquired company/division together meet the eligibility and technical evaluation criteria, their combined capabilities should be considered to ensure a fair assessment of the bidder's potential. **Industry Practice & Precedents:** Many tenders allow for the	Law of Land is implied. i.e., The Company related act 1956/2013 in INDIA, partnership, hon'ble court orders and statutory authority related to mergers and acquisitions .

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					experience and credentials of acquired entities to be counted towards eligibility, ensuring fair competition and allowing experienced market players to participate effectively. **Encouraging Market Growth & Investment**: Supporting acquisitions and business consolidations by recognizing their credentials promotes industry growth, investment, and business continuity.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1215	27	3.1.1 Eligibility Criteria:	Eligibility Criteria: The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	We request addition of this clause : A bid submitted by a Bidder who has acquired a Company/ Division of a company/100% owned subsidiary company shall also be considered for evaluation if the eligibility and technical evaluation criteria. We request change in the supporting documents : Copies of Purchase Order, completion/ Go-live certificate or partial completion certificate complying to the clause requirement from client to be enclosed along with Technical Bid. OR If the bidder, its group company, or	Inclusion of Bids from Acquired/ Subsidiary Companies Justification: In many cases, business acquisitions and mergers lead to the transfer of technical expertise, resources, and capabilities to the acquiring company. Allowing bids from companies that have acquired another firm (or its division) ensures that the experience and competencies gained through such acquisitions are not disregarded. This approach aligns with industry best practices, allowing for fair competition while maintaining the eligibility and technical evaluation criteria. Modification in Supporting Document Requirements Justification:	Law of Land is implied. i.e., The Company related act 1956/2013 in INDIA, partnership, hon'ble court orders and statutory authority related to mergers and acquisitions .

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
			Supporting Documents: Copies of Purchase Order, completion/ Go-live certificate or partial completion certificate complying to the clause requirement from client to be enclosed along with Technical Bid.	its subsidiary is a Telecom Company, the bidder should submit a self-certification detailing the NOC and the number of networks monitored for various customers.	The existing requirement limits proof of experience to purchase orders and completion certificates, which may not fully reflect the capabilities of telecom companies with extensive NOC and network monitoring experience. Telecom companies operate large-scale Network Operation Centers (NOCs) and monitor numerous networks across various clients. However, such operations are often ongoing, without formal go-live certificates. A self-certification mechanism for telecom companies allows them to demonstrate their capabilities effectively while maintaining transparency and accountability. This change ensures	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
					inclusivity of experienced telecom firms without diluting the eligibility criteria.	

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1216	-	Data Tiering	· Offered Storage array shall be able to tier NVMe SSD and SAS/NL- SAS Drives in a single pool for optimizing performance if required.	· Offered Storage array shall be able to tier NVMe SSD and SAS/NL- SAS Drives in a single pool for optimizing performance if required.	Since this requiment is for backup , then please explain the role of NVMe SSD's , also if NVMe SSD's are required then it is not mentioned in capacity , it is only asked in NL-SAS drives.	1. Repeated query. Functional capacity is explicitly mentioned. 2. Responded with intend of wider participation at multiple places.
1217	69	**4.8 Carrier Grade NAT / 4**	• The router shall support traffic classification, congestion management, traffic conditioning, hierarchical QoS policies and various other security features to prevent network attacks and vulnerabilities. • The router shall support access control lists to filter traffic based on parameters, per-user authentication, authorization and accounting. • The router shall support multicast, routing and protocols	• The firewall/router shall support QoS policies i.e. traffoc rate limiting and various other security features to prevent network attacks and vulnerabilities. • The firewall/router shall support access control lists to filter traffic based on parameters like IP addresses, protocols,users and ports. • The firewall/router shall support multicast, routing and protocols	Specific router capabilities mentioned.	Repeated query. Responded with intend of wider participation at multiple places. Pl go through.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1218	94	Functionality/Point 1	End point protection software shall be single agent software for NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates	**Change clause to below** End point protection software shall be single agent or dual agent from same OEM For NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates.	As there are multiple functionalities asked in the Clause hence relaxing the clause from single agent to dual agent from same OEM as suggested will allow maximum and broader participation	Repeated Query. Responded with intend of wider participation.
1219	27	3.1.1, Pt 5	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project please refer the definition mentioned above .	All the OEM products including software components must have proven deployment and commissioning with 2 clients in this RFP in past 7 years including the current year in India or Abroad in Goverenment/PSU's /Telecom Service providers (Tier-1/Class-A/NLD/ILD/Public Listed Company as	OEM having experience is more important, where they get such experience (India/Abroad) should not be that critical to qualify the OEM	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				on date of openning of tender)		
1220	31	3.2.1, Pt 2 d	The solutions of OEM must provide at least one reference case demonstrating GIS led support for more than 20,000 KM fiberization in any Government, PSU, pubic listed company or Telco- 5 Marks	The solutions of OEM must provide at least one reference case demonstrating GIS led support for more than 7,000 KM fiberization in any India and Abroad Government, PSU, pubic listed company or Telco - 5 Marks	For Start-ups (recognized by Department of Industrial Policy and promotion, Ministry of Comerce and Industry) only 1/3 of value as mentioned above is requred.	As per RFP
1221	31	3.2.1, Pt 3 h	The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 network elements in any Government, PSU, Bank/ pubic listed company or large-scale IP network- 5 Marks	The solutions of OEM must provide at least one reference case demonstrating support for more than 17,000 network elements in any India and Abroad Government, PSU, Bank/ pubic listed company or large-scale IP network	For Start-ups (recognized by Department of Industrial Policy and promotion, Ministry of Comerce and Industry) only 1/3 of value as mentioned above is requred.	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1222	31	3.2.1, Pt 5 d	The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 Customers in any Government, PSU, Bank/ pubic listed company or large-scale IP network. Presentation to be done for Education department live connections- 3 Marks	The solutions of OEM must provide at least one reference case demonstrating support for more than 17,000 Netwrok elements in any India and Abroad Customers in any Government, PSU, Bank/ pubic listed company or large-scale IP network. Presentation to be done for Education department live connections	For Start-ups (recognized by Department of Industrial Policy and promotion, Ministry of Comerce and Industry) only 1/3 of value as mentioned above is requred.	Pls see revision
1223	119	Bullet 2 under Note	CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value	Stands deleted	This has no relavance as 30% of project value is paid over 7 years	As per RFP
1224	118	Submission of PBG	T + 3 Weeks (T = Date of award of Nprocure contract/LOI) Payment - NIL	T + 3 Weeks (T = Date of signing of contract)	-	As per RFP
1225	118	a. Project kickoff b. Technical architecture…	T + 3 Weeks (T = Date of award of Nprocure contract/LOI) Payment - NIL	T + 3 Weeks (T = Date of signing of contract)	-	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1226	118	Demonstration of prototype /screen/functional work flow of GIS and NMS as per RFP	T + 5 Weeks - 10% of project value	T + 6 Weeks - 10% of Product value (product value = Product + 7 years warranty)	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP
1227	118	Delivery of Hardware for IT Infra and Network infra	T + 6 Weeks - 20% of project value	T + 10 Weeks - 30% of Product value	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP
1228	118	Demonstration of finished software for GFGNL on Bidder's cloud	T + 10 Weeks - 10% of project value	T + 14 Weeks - 10% of Product value	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1229	118	Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru	T + 15 Weeks - 20% of project value	T + 20 Weeks - 10% of Product value	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP
1230	118	Successful completion of FAT, completion of	T + 17 Weeks - 10% of project value	T + 22 Weeks - 10% of Product value	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
		training and Go-live				
1231	119	Operations & Maintenance	7 years from go-live - 30% of project value	7 years from go-live - 30% of Product Value as equated quarterly payments, at the end of each quarter from go-live	There is no project value, financial bid has product value (with 7 years warranty) and manpower value	As per RFP
1232	119	Manpower for O&M Phase	Day 0 from go-live - Man month Payment based on calculation on discovered cost on Quarterly Basis	Day 0 from go-live - Paid monthly after deduction of manpower relted penalty (if any)	Monthly, quarterly written in same sentence was creating confusion hence suggested correction.	As per RFP

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1233	57, 63	4.3, 4.6	Next general Firewall, NIPS	Merge NIPS with Next Generation Firewall and include URL Filtering	Merging NIPS with NGFW streamlines security operations by consolidating threat management in a single platform. This integration enhances the firewall's capability to detect and prevent intrusions in real-time while managing web access through URL filtering as all the components shall require update to their software. Offcourse, throughput & related configuration will be enhanced	We have specified dedicated items for specific purposes. The combined functionality in one or multiple boxes is allowed strictly in condition of combined performance including enablement of all purposes and all licenses without any cost to GFGNL and without any degradation in totality and individually. The objective is wider participation and to meet overall purpose and solution. The deduplication is expectation from SI. With this principle, here, the main purpose of device/devices are well established at individual and in totality as well. To derisk upon disqualification merely on ground of minor numeric values, a 10% tolerance is allowed in general for product fitments in case of participatory constraints in real sense and promoting wider participation. The intended misuse of this relaxation just for cost savings is good reason for disqualification of entire bid. Hence, SI may do proper due diligence at his stage of evaluation before the bid submission. 1. The design of security architecture, supply of quality and reputed products for running the NOC in a secured manner is the prime responsibility of capable bidder. As part of the scope of work, we have indicated security products with high payouts to successful bidder for security compliances including quarterly VAPT for proactive and preventive measures in the larger interest of fulfillment of purpose of NOC. The bidders are advice to do proper due diligence while choosing security products. 2. It is expected that bidder shall design and implement security architecture and shall be expert to derive security strength of the product, writing scripts for preventions and ability to run and manage the underlaying network of Bharatnet and NOC components efficiently in most secured manner with best of security practices.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1234	94	4.19	End point protection of VMs	Should be upgraded to XDR	Upgrading to XDR offers advanced capabilities, including continuous monitoring and response to advanced threats at the endpoint level, crucial for protecting critical infrastructure. Maintain your own data lake by merging other components present like DDOS, firewall etc. & run co-relation in single data lake which helps a ton towards robust security posture	The purpose is wider competition and for that general principles have been laid. The OEM may provide higher solution without additional cost. It can not be limitation for qualification for others.
1235	76	4.12	AAA server	Current specifications are leading to IAM which is like posture management, but considering TRAI guidelines and strict RBAC, PAM should be considered instead of AAA (IAM)	PAM provides more granular control over privileged accounts and enforces the principle of least privilege, which is crucial for meeting stringent regulatory compliance requirements and enhancing security which shall be important from TRAI standpoint	IAM or PAM are allowed including equivalence of functionalities of the respective technologies subjected to TRAI GoI guideline.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1236	-	3.1.1 Eligibility Criteria: Page 27.	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project please refer the definition mentioned above .	OEM to have a proven and extensive deployment history, which is essential for demonstrating the solution's scalability and capability to operate effectively in large, complex environments. This includes at least one deployment specifically for OpenShift and OpenStack monitoring, ensuring compatibility with modern infrastructure and cloud-native technologies. Therefore, we kindly request that the clause be amended as follows: **"The proposed EMS/NMS solution must have documented deployment references where it**	-	Pls see revision

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				has successfully monitored and managed over 15,000 nodes across atleast three deployments in Government, PSU, or large enterprise environments., and at least one must specifically include OpenShift and OpenStack monitoring to validate the product's capabilities and credentials."		
1237	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 55.	OSS tool should be certified TEC-GR-IT-NMS-003-01-NOV-15, comprehensive eTOM coverage	The current TEC-GR specifications primarily focus on older generation platforms. To ensure that the requirements are aligned with the functional needs of this tender, we kindly request that only the relevant specifications be considered, while making all other clauses optional. Therefore, we	-	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				suggest amending the clause as follows: **"The OSS tool should comply with the relevant standards outlined in TEC-GR-IT-NMS-003-01-NOV-15, applicable to the current requirements."**		
1238	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 47.	Auto generation of configuration for new nodes and auto Integration.	Auto-generation of configuration is generally a device-level functionality, while NMS/EMS systems are designed to provide centralized monitoring and management. To align with industry best practices, the solution should incorporate intelligent configuration management, enabling automation at scale, as well as efficient backup and restoration of	-	1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				network configurations. Therefore, we kindly request that the clause be amended as follows: **"The EMS should conduct the monitoring and management with the intelligent configuration of multiple network switches and routers. Should have Centralized Automation at Scale with Ansible-powered Network Automation. Intelligent Network Device Configuration Management should be provided for control of the network infrastructure by effortlessly performing configuration backups, compare network configurations to**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				ensure compliance with regulatory standards. It should allow to perform configuration backup of routers, switches, comparison of configuration across network devices, line-by-line comparison and in-line comparison. It should allow to define playbooks for configuration tasks , should perform configuration on single device as well as host group."		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1239	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 48.	Automated Deployment (AC): New nodes should be auto configured with minimal engineer intervention.	Auto-generation of configuration is generally a device-level functionality, while NMS/EMS systems are designed to provide centralized monitoring and management. To align with industry best practices, the solution should incorporate intelligent configuration management, enabling automation at scale, as well as efficient backup and restoration of network configurations. Therefore, we kindly request that the clause be amended as follows: **"The EMS should conduct the monitoring and management with the intelligent configuration of**	-	Pls see preceding response for wider participation

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				multiple network switches and routers. Should have Centralized Automation at Scale with Ansible-powered Network Automation. Intelligent Network Device Configuration Management should be provided for control of the network infrastructure by effortlessly performing configuration backups, compare network configurations to ensure compliance with regulatory standards. It should allow to perform configuration backup of routers, switches, comparison of configuration across network devices, line-by-line comparison and in-line comparison. It		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				should allow to define playbooks for configuration tasks , should perform configuration on single device as well as host group."		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1240	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 51.	Automated Deployment (AC): New nodes should be auto configured with minimal engineer intervention.	Auto-generation of configuration is generally a device-level functionality, while NMS/EMS systems are designed to provide centralized monitoring and management. To align with industry best practices, the solution should incorporate intelligent configuration management, enabling automation at scale, as well as efficient backup and restoration of network configurations. Therefore, we kindly request that the clause be amended as follows: **"The EMS should conduct the monitoring and management with the intelligent configuration of**	-	Repeated Query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				multiple network switches and routers. Should have Centralized Automation at Scale with Ansible-powered Network Automation. Intelligent Network Device Configuration Management should be provided for control of the network infrastructure by effortlessly performing configuration backups, compare network configurations to ensure compliance with regulatory standards. It should allow to perform configuration backup of routers, switches, comparison of configuration across network devices, line-by-line comparison and in-line comparison. It		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				should allow to define playbooks for configuration tasks , should perform configuration on single device as well as host group."		
1241	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 48.	Automated traffic diversion to bypass degraded links.	Automated traffic diversion, real-time bandwidth optimization, and path computation and optimization are typically functionalities associated with individual devices. On the other hand, an NMS primarily focuses on monitoring, fault detection, performance management, and	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				traffic analysis. In light of this distinction, we kindly request that this clause be excluded from the NMS scope and instead be considered as part of the device functionality.		
1242	-	4.2 Operational Visibility Platform (NMS+ OSS + BSS+ Network visibility): Page 48.	Real-time bandwidth optimization across network segments.	Automated traffic diversion, real-time bandwidth optimization, and path computation and optimization are typically functionalities associated with individual devices. On the other hand, an NMS primarily focuses on monitoring, fault detection, performance management, and traffic analysis. In light of this distinction, we kindly request that	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				this clause be excluded from the NMS scope and instead be considered as part of the device functionality. So, we kindly request to amend this clause as below: **"Bandwidth & Traffic monitoring across networks"**		
1243	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 48.	Solution should support three (min.) and ten (max.) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target.	The clause regarding 'parallel path traces' pertains to ensuring efficient and reliable path discovery and monitoring of network performance. However, for effective and proactive network monitoring, it is crucial to have a comprehensive and automated network topology that includes detailed relationships between devices, interfaces, and their	-	Pls see preceding response for wider participation

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				respective statuses. Therefore, we kindly request that the clause be amended as follows: **"The proposed solution must provide the complete view of the Network Topology. It should have the ability to include the network elements and custom topology. Should have automated network topology and host Discovery without manual mapping of network, empowering with real-time visibility into network infrastructure with up-to-date network insights. The topology should provide details of neighbors, neighbor IP, neighbor interface, statistics, device vendor, model. The**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				topology should show Traffic utilization, interface status & details on hovering the mouse over the link/interface."		
1244	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 51.	Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target.	The clause regarding 'parallel path traces' pertains to ensuring efficient and reliable path discovery and monitoring of network performance. However, for effective and proactive network monitoring, it is crucial to have a comprehensive and automated network topology that includes detailed relationships	-	Repeated query

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				between devices, interfaces, and their respective statuses. Therefore, we kindly request that the clause be amended as follows: **"The proposed solution must provide the complete view of the Network Topology. It should have the ability to include the network elements and custom topology. Should have automated network topology and host Discovery without manual mapping of network, empowering with real-time visibility into network infrastructure with up-to-date network insights. The topology should provide details of neighbors, neighbor IP, neighbor interface, statistics,**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				device vendor, model. The topology should show Traffic utilization, interface status & details on hovering the mouse over the link/interface."		
1245	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 48.	The proposed solution should be able to clearly visualize the Hop by-Hop visibility of the Underlay Network at a granular level Sub Second) for Identifying clear problematic sections on the Glass pane view	The original clause's requirement for 'sub-second' visibility is highly specific, as the level of granularity provided by a network monitoring solution typically depends on both the monitoring frequency and the overall performance of the network. Therefore, we kindly request that the clause be amended as follows:	-	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				"The proposed solution should be able to clearly visualize the Hop by-Hop visibility of the Underlay Network for Identifying clear problematic sections on the Glass pane view."		
1246	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 49.	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	The original clause regarding 'synthetic network tests' pertains to testing network performance by simulating traffic between two points, which is more applicable to specialized network testing tools than to a Network Management System (NMS). NMS solutions primarily focus on real-time monitoring of network traffic patterns to gather actionable insights, along with comprehensive FCAPS functionality.	-	The functional specification has been specified. It is the SI responsibility to provide the same

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				Therefore, we kindly request that the clause be amended as follows: **"The tool should have Network Traffic Analysis based upon netflow for network switches and routers. Traffic monitoring should collect and analyze network traffic patterns to provide with real-time traffic utilization and bandwidth usage. The module should monitor network flows to identify traffic like Top Talkers, IP to IP traffic, monitor the bandwidth The tool should Dive deep inThe tool should identify and display traffic details such as top hosts, top protocols, top applications, and top talkers consuming the**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				most bandwidth. It should also provide an option to view live traffic details for real-time analysis.to network traffic patterns, gain actionable insights."		
1247	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 52.	The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.	The original clause regarding 'synthetic network tests' pertains to testing network performance by simulating traffic between two points, which is more applicable to specialized network testing tools than to a Network Management System (NMS). NMS solutions primarily focus on real-time monitoring of	-	The functional specification has been specified. It is the SI responsibility to provide the same

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				network traffic patterns to gather actionable insights, along with comprehensive FCAPS functionality. Therefore, we kindly request that the clause be amended as follows: **"The tool should have Network Traffic Analysis based upon netflow for network switches and routers. Traffic monitoring should collect and analyze network traffic patterns to provide with real-time traffic utilization and bandwidth usage. The module should monitor network flows to identify traffic like Top Talkers, IP to IP traffic, monitor the bandwidth The tool should Dive deep inThe tool should identify and display**		

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				traffic details such as top hosts, top protocols, top applications, and top talkers consuming the most bandwidth. It should also provide an option to view live traffic details for real-time analysis.to network traffic patterns, gain actionable insights."		
1248	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 50.	The proposed tool must provide a structured, Latest ITIL compliant problem management framework, ensuring effective issue tracking, resolution, escalation, and reporting. It should support integration with incident, change, and **configuration management** while offering automated notifications, advanced analytics, and stakeholder communication capabilities.	Aligning with industry standards and in accordance with the tender requirements, the ITIL v4 certification for at least six core ITSM processes, as best practices for service management, is deemed sufficient. Therefore, we kindly request that the clause be amended as follows: **"The proposed**	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				ITSM tool should have ITIL v4 Axelos certification for at least the following six processes: Incident Management, Service Request Management, Problem Management, Change Management, Knowledge Management, and Service Level Management."		
1249	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 52.	Automated Security Hardening: Enforcing NTP, AAA, SNMP, SYSLOG, and firewall security policies.	Security hardening, including the enforcement of policies for NTP, AAA, SNMP, SYSLOG, and firewalls, is generally considered a part of network and device security management functions. Therefore, we kindly request that this clause be excluded from the NMS scope.	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1250	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 52.	Audit & Remediation: Continuous compliance checks with auto remediation.	Using playbook-based remediation for continuous compliance checks ensures that configuration changes are automated, consistent, and repeatable across the network. The ability to define playbooks allows network operators to codify configuration tasks, whether for individual devices or entire host groups. So we kindly request to ammend this clasue as below: **"Continuous compliance checks with playbook-based remediation. It should allow defining playbooks for configuration tasks, and should perform configuration on single devices as**	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				well as host groups."		
1251	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 53.	Patch Management: Automating security patches across infrastructure.	Patch management is typically a standalone solution designed to handle the patching of various infrastructure components, rather than being part of the NMS. The NMS, on the other hand, primarily focuses on network configuration management tasks, such as firmware image uploads/downloads, OS uploads/downloads, and maintaining an	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				OS library. Therefore, we kindly request that the clause be amended as follows: **"NMS should provide network configuration management, including firmware image upload/download, operating system (OS) upload/download, and maintaining an OS library for efficient management."**		
1252	-	4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): Page 53.	The platform must include a CMDB with asset lifecycle management, software license metering, and patch evaluation. Historical data retention must align with regulatory guidelines	Patch management, software license management, and asset lifecycle management are typically handled by separate solutions and are not part of the NMS. Therefore, we kindly request that the clause be amended as follows: **"The solution should allow**	-	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through the scope

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				management of asset details including warranty, expiration, and acquisition of assets/inventory. It should also track warranty expiry and provide notifications. Additionally, the system should allow for the definition of different asset statuses such as In-use, Repaired, In-Store, and Expired to ensure efficient asset management throughout their lifecycle."		of work, functional aspects, supportive technical language for better understanding.

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1253	-	-	Request for Addition	According to the latest DPIIT guidelines and notifications, compliance with the 'Make in India' requirements must be ensured. The proposed OEM for the NMS should meet the following criteria: 1. Intellectual Property Rights (IPR) must be held in India. 2. The OEM must facilitate the validation of IPR and source code copyright through copyright.gov.in to verify authenticity, in line with DPIIT guidelines. Additionally, the proposed NMS/EMS tool should be listed as an approved product on the Trusted Telecom Portal (TTP).	-	While addressing the risk of eliminations on minor grounds, we are reiterating the below general principles of governing ease in evaluation and ease of doing business to de-risk from proprietary terminology and falsification perception leading towards elimination of competition. 1) Tenderer want wider competition, MII, ease in technical terminologies. 2) The default applicability of DoT directives for technical and regulatory aspects and DPIIT directives for make in India. 3) Tenderer want adoption and implementation of Make in India policy and latest notifications in letter and spirit. 4) The TEC GRs are the fabric of functionality and latest TEC GRs is the default applicability. 5) Ease in technology terminologies. The equivalence of any standard, proprietary words / monopolized ask, workaround minor ports, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds without any additional cost to GFGNL and without diluting functional deliverables."

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
1254	-	-	Request for Addition	Given the criticality and importance of the solution, it is imperative to ensure that the tool holds mandatory certifications from CERT-In, OWASP, and SANS. We request that the following be considered: 1. The proposed NMS solution should have a qualified certification from a government agency, issued by one of the CERT-IN empanelled Information Security Auditing organizations for testing and certification/clearance. 2. The proposed EMS solution should possess a valid and genuine CMMI L3 certificate to streamline processes efficiently, promote	-	Pls see previous response

SN	Page No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Reason by Bidder	Response by GFGNL
				productivity, and reduce risks in software, product, and service development. The OEM should facilitate the validation of the CMMI L3 certificate through the CMMI Institute's PARS portal.		

==========End Of Document==========

Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center -GFGNL

Issued by:
Gujarat Fibre Grid Network Limited
Reference No: **GFGNL/GFG/e-file/263/2025/0016/NOC**

09th April 2025

Issued By:

Gujarat Fibre Grid Network Limited (GFGNL)

A Government of Gujarat Company

Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Revised clause for Bid evaluation:

The bids would be processed in the following sequence:

Stage-I: Tender Fee, EMD, Integrity pact, Authorization.

Stage-II: Bidder's qualification stage:

The purpose of this stage is to examine financial strength, execution credentials, quality certifications, Land border regulations and etc based on submissions as evidentiary proofs specified in the Pre-qualification criteria section. Any shortfall in the specified benchmarks is a good reason to disqualify bidder at this stage.

Stage-III: Bid qualification stage:

The purpose of this stage is to examine available bid capacity related commitments for Gujarat, better quality components, Contractual commitment towards early project rollout for before time delivery of project, , Architecture, GIS, NMS, OSS, BSS, additional creativity and offerings without additional charges.

It is mandatory for the bidder to provide legitimate documentary proofs / committal undertakings for claiming the score as specified in the technical qualification criteria section. Any higher commitment shall be revised in the SLA and timelines part of the contract unconditionally.

It is mandatory to score minimum 60% in each criteria section and overall score of minimum 75% for qualifying into final stage.

Any shortfall to the minimum specified score is a good reason to disqualify bidder at this stage.

Stage-IV: Financial stage:

Least cost method is applied.

If L1 Bidder is not agree or not qualify at later stage to execute the project for any reason, Tenderer may call L2 Bidder to match the price of L1. If L2 agree to match the price of L1, tenderer may award the contract. The same process may be followed for remaining qualified Bidders. Tenderer may cancel this procurement process at any time prior to a formal written contract being executed by or on behalf of the GFGNL without giving any reason. This RFP supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

In case of any ambiguity, GFGNL may download the files from the portal and do the offline evaluation as per the parameter defined in tender document.

Revised TECHNICAL QUALIFICATION CRITERIA

Notes-

1. The bidder(s) has to submit the valid and legitimate documents for claiming the score including corresponding formula.
2. A rank stand for 100% weightage to be considered for scoring in below evaluation table. Subsequently, B rank stands for 75% weightage and C rank stands for 60% weightage.

S. No.	Criteria	Evaluation	Documentary Proof	Score
1	Bid capacity	No. of network nodes in WAN, managed and monitored in last 8 years (7 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank No. of Clientele in last 8 years (3 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank	— The comparative ranking among all the bid participants will be considered for each of the parameters.	10
2	Offered product portfolio	Quality products / components (Mentioned in Part-A Financial bid components of RFP) — Past credentials in terms of market share featured in latest publication (3 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank — Additional quality certification issued by any Govt./ National associations (2 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank	— The comparative ranking among all the bid participants will be considered for each of the parameters. — Additional quality certification over and above asked in the RFP	5

S. No.	Criteria	Evaluation	Documentary Proof	Score
		Note - 2 additional marks will be given to Make in India (MII) software solution.		
3	Rollout Commitment for software	**Rollout commitment including final functionalities of GIS and NMS, commissioning for live use in BharatNet,** A. Less than 09 weeks B. Less than 12 weeks **C.** Maximum 15 weeks	— Legitimate undertaking as part of revision in the contract for penalty calculation	10
4	Rollout Commitment for entire project including GFGNL cloud	**Rollout commitment,** A. Less than 15 weeks B. Less than 17 weeks **C.** Maximum 18 weeks	— Legitimate undertaking as part of revision in the contract for penalty calculation	5
5	Architecture	**Factoring of below critical aspects as part of clarity in technical architecture and completeness in overall solution.** I. High availability II. High performance **III.** DC-DR high turnaround aspects **IV.** Security architecture	— Legitimate undertaking as part of better offerings, inclusion of missing part for attaining architecture objectivity without any additional cost to GFGNL.	15
6	GIS	**Demonstration of prototype/readiness to meet technology led Governance in GIS** a) Project management- 3 Marks b) Digital measurement book- 3 Marks c) Virtual inspection- 4 Marks d) The solutions of OEM must provide at least one reference case demonstrating GIS led support for more than 20,000 KM fiberization in any Government, PSU, public listed company or Telco- 5 Marks	— Proof of concepts	15

S. No.	Criteria	Evaluation	Documentary Proof	Score
7	NMS, OSS and BSS	Demonstration of prototype/readiness to meet technology led Governance in NMS, OSS and BSS **NMS, OSS Part:** a) Service provisioning automation level- 1 Mark b) Network scanning and KPIs- 1 Mark c) Digital SLA measurement- 1 Mark d) Dashboard for MD, HQ, District, Client- 2 Marks e) High performance architecture for speedier reports and real time calculations. -1 Mark f) Integration convenience/understanding as per telco practice by API/NE of all type of elements in BharatNet.-1 Mark g) Any other important functionality to be shown. - 1 Mark h) The solutions of OEM must provide at least one reference case demonstrating support for more than 15000 network elements in any Government, PSU, Public listed company or large-scale IP network- 2 Marks **BSS Part:** a) UX (User Experience), Navigation, ordering and service creation. -1 Mark b) Integration of BSS with OSS in NMS- 1 Mark c) Optimization of licenses in BSS to meet current requirements and future	— Proof of concepts	15

S. No.	Criteria	Evaluation	Documentary Proof	Score
		scalability with reduce licensing cost. - 1 Mark d) The solutions of OEM must provide at least one reference case demonstrating support for more than 15000 Customers in any Government, PSU, Public listed company or large-scale IP network. Presentation to be done for Education department live connections- 2 Marks		
8	Presentation	**Presentation: -** a) Previous Project Handling Experience in high performance unified deployments. (NOC, Data center, NMS, Network GIS) -3 Marks b) Industry deployment use cases in quoted software products. - 3 Marks c) Performance visibility – ICT and service and high availability commitment. - 3 Marks d) Technology led governance, data driven supervision, virtual inspection and management dashboard. - 3 Marks e) Proposed Team size during execution (On site and off site) including minimum profile in our project (this will be part of contract). *-4 Marks f) Proposed Team size during professional O&M (On site and off site (institutional support)) including minimum profile in our project (this will be part of contract). *- 4 Marks * **Note:** The best proposal in terms of size and profile will be given highest marks and there after rest will be given marks on percentile basis	— Legitimate undertaking as part of commitment for additional offering	20

S. No.	Criteria	Evaluation	Documentary Proof	Score
9	Additional Offering	Value added offering over and above the ask of RFP without any additional charges. I. Use of Licenses, II. higher capacity in storage/ No of cores, III. manpower, IV. contract duration, V. offering of AI VI. Any other significant creative offering On fulfillment of above offering, A. Any 5 offering out of 6 B. Any 4 offering out of 6 **C.** Any 3 offering out of 6	— Legitimate undertaking as part of commitment for additional offering	5
	Total Score			**100**

Illustration:

Evaluation (for each Package)	Documentary Proof	Score
No. of network nodes in WAN, managed and monitored in last 8 years (7 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank No. of Clientele in last 8 years (3 score) A. Top 2 rank B. Top 3 to 5 rank C. For remaining rank	— The comparative ranking among all the bid participants will be considered for each of the parameters.	10

If three bidders have participated in bid, and

Bidder-1 has submitted experience of 5000 nodes and 7 clientele,

Bidder-2 has submitted experience of 7000 nodes and 6 clientele,

Bidder-3 has submitted experience of 6000 nodes and 5 clientele,

then,

Bidder-2 and 3 will get A-rank and Bidder-1 will get B-rank in no. of nodes experience,

Bidder-1 and 2 will get A-rank and Bidder-3 will get B-rank in no. of clientele.

And score for each bidder will be as per below,

Bidder-1: (7 x 75%) + (3 x 100%) = 5.25 + 3 = 8.25 score

Bidder-2: (7 x 100%) + (3 x 100%) = 7 + 3 = 10 score

Bidder-3: (7 x 100%) + (3 x 75%) = 7 + 2.25 = 9.25 score

==========End Of Document==========

Corrigendum-VI

Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center for ABP (Phase-III)-GFGNL in Gujarat

Issued by:
Gujarat Fibre Grid Network Limited
GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016/NOC

05th May 2025

Issued By:

Gujarat Fibre Grid Network Limited (GFGNL)

A Government of Gujarat Company

Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Corrigendum

The Bidders are requested to take note of the following changes made in the RFP document, which are to be considered while submitting the RFP response. They shall be presumed to have done so and submitted the RFP response / bid accordingly.

• This Corrigendum shall be the part of the RFP documents / process.

• All items specified in this Corrigendum supersede relevant items to that effect as provided in the original RFP documents. All other specifications, terms and conditions of the original RFP document shall remain unchanged.

• Text with strikethrough means it is deleted.

Fact sheet:

#	Particular	Details
9	Last date for submission of Bid/proposal	~~04/04/2025,11/04/2025,17/04/2025 at 06:10 pm,~~ ~~28/04/2025~~ ~~08/05/2025~~ →22/05/2025 at 6:10 pm

Pre-bid Query Response

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
1	119	Bullet 2 under Note	CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value	70% of project payment are done till go-live and 30% over 7 years against CAMC. Then CAMC can't be 7% of CAPEX	Paying 70% of overall project value against go-live leave 30% for balance period, including manpower (project value = capex + CAMC + manpower) and the CAMC has to be 49% of CAPEX.. So whole maths doesn't workout. Either keep Manpower separate from project value (nothing else changes) OR change the %ges	Pls see revision
2	125	5.41	Payment term - %age of project value of different milestones	The financials comprise of Product (including 7yr wty, manpower and 3yr price). We assume project value is the product value with 7 year warranty. Is the understanding correct?	No where project value is defined, so necessary to capture it for clarity when commercials are asked under 3 heads	Pls see revision
3	126	Milestone 9	Manpower for O&M phase - Manmonth payment on quarterly basis	Request for monthly payment term for manpower instead of quarterly.	Since the resources are paid salary on monthly basis	Currently GFGNL is handling multiple O&M contracts and in all the contracts, the standard practice is quarterly payments for ease in processing and managing the payment span. This has found good for GFGNL and partners.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
4	112 and 113	5.27, 5.32	5.27 - Indemenification 5.32 - Patent rights, copy right and IPR The query is responded in Sr no 1197 but probably its taken differently, as visible from the responde. The matter is that indemnification is typed at 2 places in section 5.27 and 5.32. Asking for removal from 5.32 is not for reducing compeition.	Request for the deletion of 5.32 OR suggested clause - *The OEM shall indemnify tenderer against all third-party claims of infringement of copyright, patent, trademark or industrial design rights arising from use of their Goods/services. In the event of any claim asserted by a third party, the OEM shall act expeditiously to extinguish such claim. If the OEM fails to comply and tenderer is required to pay compensation to a third party resulting from such infringement, the OEM shall be responsible for the compensation to the Tenderer including all expenses, court costs and lawyer fees.* *Bidder will facilitate and support GFGNL in the above claims from OEMs*	Section 5.27 is pragmatic but section 5.32 is exactly opposite and over protective. All OEMs give undertakings in the name of tenderer, they are also the bidders (though not front ending) so are qually liable for their portion of solution and hence responsible for their acts of infringement in their quoted products. Bidder has no means of verifying infrigments, Bidder can facilitate and support the tenderer for claming damages due to infringement	Pls see revision
5	155	7.7 SLAs for patch managem ent	There are various slabs given for penalty for not meeting 4 categories of patch management (Critical, high….).	There are penalties on missing fixes on vulnerabilites in 7.6; then this section will create conflict. Either of these 7.6 (Pt 3) or 7.7 should be kept	Other than chosing one of two penalties 7.6/7.7 for patches; the penalty should be waived off for delay in fixing patches for those where systems may get impacted or patches are not getting right feedback from global communities or where tenderer approval is required.	Pls see revision, Reduction on % of Penalty of patch management and system upgrade

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
6	45	Page 45 EMS & NMS Integration	All network elements and routes must be integrated with existing GFGNL NMS	Do you have any NMS solution if yes please name it or you need Fresh NMS solution to monitor the Router,Switch, Firewal		Pls go through the specific section related to NMS containing the purpose and objectivity. It is to clarify that the NMS sought in this RFP has no correlation with existing NMS except migration aspect for unlocking participation for non existing NMS.
7	45	Page 45 EMS & NMS Integration	Bidder to provide perpetual software license for entire solution including EMS.	Are you looking for ITSM solution for auto ticketing ? And server monitoring solution as well?		Pls refer entire functionality requirement mentioned in Tech spec 4.2. point 3(Helpdesk & Customer Issue Management & Problem Management)

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
8	45	Page 45 EMS & NMS Integration	Additional points recommended for Fresh NMS and EMS solution 1]To ensure the mature security standard of proposed EMS solution, SI must ensure that the proposed EMS solution OEM is ISO 27034 certified from one of the following certification agencies: Schellman/ KPMG/ PwC/ Ernst & Young/ Deloitte. Documentary proof must be provided at the time of submission. 2]The proposed solution must be Information Security Management System certified with ISO/IEC 27001:2013 and ISO 9001 certificates. 3]The NMS tool shall be able to discover IPv4 only, IPv6 only as well as devices in dual stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses. 4] NMS shall be able to capture, track & analyse	Request you to please add points for fresh NMS and EMS solution points		Pls refer the Eligibility criteria where such certification asked from bidder.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc. 5]TheEMS solution should have IT Service Management documentation/ guidelines in-built based on ITIL V4 best practices and must be People Cert Gold certified on at least 9 ITILv4 processes i.e., Incident Mgmt., Knowledge Mgmt., Service Request Mgmt., Service Catalogue Mgmt., IT Asset Mgmt., Change Enablement, Service Configuration Mgmt., Problem Mgmt., Release Mgmt., etc. The certification copies to be submitted. 6]The proposed EMS solution should be accessible from a single pane of glass for KPI insights across the entire IT environment. This dashboard will provide service status, performance view, response-time data etc based on role-based access for streaming metrics across systems, applications, networks, topology & event data, the			

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			solution must be FIPS 140-2 compliant, which ensures that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. 7]The proposed EMS solution should be built on modern container technologies deployable on containerized (like Docker, Kubernetes) mode. The solution should either support built-in Kubernetes technology or Bring Your Own Kubernetes (BYOK) platform provided by the bidder.			

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
9	86	Server Interface	Serial Port, 2 x USB 3.2 Gen 1Port,	kindly modify the clause as "-Serial Port, 2 x USB 3.0/3.2 Gen 1 Port,"	Kindly modify for wider participation as both have same transfer speeds.	Pls see revision
10	86	Server - Network Interface	"• infiniband Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter"	"Please revise this for wider OEM participation as it is restritcing us to participate: ""• infiniband / Ethernet Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter"""	Pls revise as it is restricting us to participate.	This is performance related ask. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.
11	88	System Security	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms,Chassis Intrusion detection option	"Please revise as some of terminology is OEM specific: ""• UEFI Secure Boot, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser,Bezel Locking Kit option/ security bezel, Support for Commercial National Security Algorithms, chassis intrusion detection option.	Pls revise as it is restricting us to participate.	Pls See revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
12	88	Server / Backup Server /	"• Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 +3 years 24 x 7 Proactive warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider or any other agency during the entire contract duration of 7 +3 years."	please change the warranty period to 5 as other components also have 5 year warranty mentioned		Since GFGNL asking for total 10 years of contract period from SI where 3 years of CAMC is to be done by SI . Extensive warranty period essential for smooth project handling.
13	95	Backup Server Interface	2 x USB 3.2 Gen1 ports or higher	kindly modify the clause as " 2 x USB 3.0/3.2 Gen 1 Port or higher,"	Kindly modify for wider participation as both have same transfer speeds.	Pls see revision
14	94	Backup server Interfaces	"• infiniband Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter"	"Please revise this for wider OEM participation as it is restritcing us to participate: ""• infiniband / Ethernet Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter"""	Pls revise as it is restricting us to participate.	This is performance related ask. However, for slight variation and fitment of product, the general tolerance of 10% +/- is acceptable.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
15	95	Backup Server System security	"• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms (CNSA), Chassis Intrusion detection option"	"Please revise as some of terminology is OEM specific: ""• UEFI Secure Boot, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser,Bezel Locking Kit option/ security bezel, Support for Commercial National Security Algorithms, Chassis INtrusion detection options"		The equivalence is allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
16	96	Backup server Embedded Remote Management and firmware security	• Server should support agentless management using the out-of-band remote management port. • Local or Directory-based user accounts with Role based access control. • Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console."	"Some of the terminologies are OEM specific please revise as below: ""• Server should support agentless management using the out-of-band remote management port. • Local or Directory-based user accounts with Role based access control. • Remote console sharing for min 2 users SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console."""	Some of the parameters are OEM specific. Hence requesting you to revise this.	The equivalence is allowed for wider participation
17	80	Core Switch	Interface & Performance: TEC GR 480060:2023	Please remove this TEC GR 48060:2023 as this is related to Telecom products while here we are adding switch for Data Center environment so please remove it for us to participate as it is restricting.	Pls remove the TEC GR as it is not applicable to a DC Switch .	~~R~~elevant TEC GR for DC level switches.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
18	81	Aggregation Switch	Functionality : TEC GR 48060:2023	Please remove this TEC GR 48060:2023 as this is related to Telecom products while here we are adding switch for Data Center environment so please remove it for us to participate as it is restricting.	Pls remove the TEC GR as it is not applicable to a DC Switch .	~~R~~elevant TEC GR for DC level switches.
19	62	4.3 Network Intrusion Prevention System (NIPS)	"• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver ~~100~~ 60 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto ~~400~~ 100 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency"	"• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver ~~100~~ 60 Gbps of real-world Intrusion Prevention System (IPS) Inspection throughput scalable upto scalable upto 140Gbps on the same box (1 RU) supporting 60M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL having minimal latency."	"The latency parameter can change based on multiple parameters like type of port , bandwidth , security configurations in the solution , load on the solution etc. therefore necessiate the changes The organization's network size and growth rate do not necessitate stacking to achieve 300 M concurrent connections/sessions. " Pls modify as suggested so as to allow us to qualify and participate.	Pls see Revision for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
20	63	4.3 Network Intrusion Prevention System (NIPS)	Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure.	Should be an on-premise standalone NIPS appliance.	This clause restricts us from participation. Hence requesting you to modify this as suggested.	Pls see Revision for wider participation
21	68	4.6 Next Generation Firewall	The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active, Active/Passive and HA clustering support.	The firewall should have minimum 4 x100/40G,4x10G/25G and 4 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active (HA clustering support) and Active/Passive.	The asked interface count is high and restricts us from participation. We request you to modify as suggested so as to allow us to participate.	Pls see revision
22	68	4.6 Next Generation Firewall	• The Appliance must handle the threat prevention throughput of minimum ~~60~~ 50 Gbps enabling security features and measured with Enterprise Mix / Application Mix traffic. • The Firewall must deliver minimum ~~80~~ 50 Gbps of IPSEC throughput from day 1. • The Appliance should support minimum New Connections per Sec of 1 million. The Application should have	"• The Appliance must handle the threat prevention throughput of minimum 80 Gbps enabling security features and measured with Enterprise Mix / Application Mix traffic. • The Firewall must deliver minimum ~~80~~ 50 Gbps of IPSEC throughput from day 1. • The Appliance should support minimum New Connections per Sec of 1 million." • The Application should have Concurrent Sessions of – 60 million from day one.	Threat prevention and IPSEC throughput can't be same.If considering 50 Gbps of IPSEC throughput(revised one) threat prevention throughput should be more.	Pls see revision.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			Concurrent Sessions of – 60 million from day one.			

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
23	69	4.6 Next Generation Firewall	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window can be schedule or automatic** **• Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV action such as allow, deny/drop,alert etc.** **• NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in**	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. **• The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware/IPS signatures and should have minimum signatures update window can be schedule or automatic** **• Should be able to perform Anti-virus /IPS scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV/IPS action such as disable, deny/drop,alert etc.** **• IPS must deliver more than 20000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect against Denial of	CDR is a functionality of email security solution and this can be achieved using email security in conjunction of NGFW which are specialized for content sanitization. This is not a primary focus of firewall. SSH inspection causes SSH traffic , breaks the connection and causes issues in regaining connection.There is no specific use case of SSH inspection. Many of the highlighted clauses are OEM specific. Hence kindly modify as per the suggested changes for better particiation and with the changes suggested the functional requirement remains same.	Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			real-time. **• IPS must deliver more than 10000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities.** • Firewall Services with Access Lists and time-based Access lists/policyto provide supervision and control. • Should protect against Denial of Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies with various categories and ability to queries a real time OEM threat intel database **• The NGFW should have both SSL and SSH Inspection capabilities"**	Service (DOS) and DDOS attacks • NGFW should be able to monitor encrypted traffic to detect APTs hiddenin SSL traffic. • The proposed firewall should have auto/schedule-based update. • The proposed solution should cater to reputation and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies with various categories and ability to queries a real time OEM threat intel database **• The NGFW should have both SSL or SSH Inspection capabilities"**		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
24	76	4.12 AAA Server	AAA Solution should be scalable enough to support added endpoints inthe network. Facility to integrate with multiple devices and gateways i.eSMS, Payment, Email ..etc.	AAA Solution should be scalable enough to support added endpoints in the network. Facility to integrate with multiple devices and gateways i.e SMS, Email ..etc.	We understand that AAA is for NOC users and devices only. Hence the asked integration with payment gateway may not be required. Hence request you to remove the same.	Pls see corrigendum II query response
25	74/ 75	CGNAT	"• The router shall support traffic classification, congestion management, traffic conditioning, hierarchical QoS policies and various other security features to prevent network attacks and vulnerabilities. • The router shall support access control lists to filter traffic based on parameters, per-user authentication, authorization and accounting. • The router shall support multicast, routing and protocols"	Pls revise as : "• The firewall shall support QoS policies i.e. traffic rate limiting and various other security features to prevent network attacks and vulnerabilities. • The firewall shall support access control lists to filter traffic based on parameters like IP addresses, protocols,users and ports. • The firewall shall support multicast, routing and protocols"	Pls modify as suggested to allow us to participate.	Pls see Revision
26	76	CGNAT	• Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., Net Flow) and the ability to detect	• Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., Net Flow) and the ability to detect deviations from normal baselines.(if required in future)	Pls modify as suggested to allow us to participate.	The equivalence is allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			deviations from normal baselines.			
27	1174	BNG	Removing specific ask for wider participation. The user plane / data plane solution should have minimum 8 Tbps switching capacity with adequate forwarding performance to meet traffic requirements. The objective is wider participation and for such minor level numeric will not be reason for disallowing products.	While GFGNL understands the functionalityof BNG, each subscriber internet traffic on the data plane will land on the BNG, which essentially means if GFGNL plans for accomodating only 100,000 subscribers being served by the BNG with each subscriber 40Mbps Bnadwidth, total traffic hitting the BNG by design would be 4Tbps Full duplex. Hence consdering scalability and best design practices, BNGshould support 8Tbps or more as data plane traffic hanling capability	Request GFGNL to maintain data plane bandwdith of 8Tbpr or above	Pls see the previous corrigendum.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
28	-	Core Router	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence, participants may go through	Routing and protocols Segment routing, SR TE, SR PCE, SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP. All these protocols mentioned are part of the IETF standards and are not proprietary in nature. GFGNL across all three RFP's have asked for Network automation, serivce automation and automated service provisioning, if a vendor does nto support these IETF functionalities in the Core Router, none of the above mentioned services or autmation is possible, Core Router at NOC being responsbile to aggagregate all the Phase I, Phase II and Phase III networks. Hnece making this clause optional will put GFGNL is big issue to complay to other functionaities asked in the RFP.	Request GFGNL to keep all these IETFdefined standards as mandatory	The equivalence is allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			the scope of work, functional aspects, supportive technical language for better understanding.			

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
29	-	4.6 Next Generation Firewall: Threat Protection	NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time.	Request to kindlly remove the clause.	Request you to please remove this clause CDR should be a dedicated component, as this clause not related to the firewall solution. As CDR is file driven, which should be for file server or respo as it provides a crucial layer of protection against file-based malware. So please remove this clause completely from the Firewall section for wider and fair participation.	Pls see revision.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
30	**3**	**Capacity & scalabiltiy**	· The Storage Array shall be offered with 500TiB (BASE- 2) capacity (260 TiB NVMe SSD + 240 TiB NL-SAS) without Dedupe and compression in RAID6 configuration or better. · Offered storage array shall be flexible on both Scale-up and Scale- out using array in-built firmware enabled clustering technology. · The storage model offered should be capable of supporting 3,00,000 or above IOPS and latency equal to or sub mili sec of response time for required IOPS from day one and it should be scalable to 6,00,000 IOPS with scale up/scale out architecture. · Storage should be able to scale 40% more capacity without adding any additional controller. · The storage system should have minimum 384GB Global Data Cache and Expandable upto 768GB. Cache memory should be delivered on DRAM; any other device or HDD should not be considered as cache.	· The Storage Array shall be offered with 500TiB (BASE- 2) capacity (260 TiB SSD/NVMe SSD + 240 TiB NL-SAS) without Dedupe and compression in RAID6 configuration or better. · Offered storage array shall be flexible on both Scale-up and Scale-out using array in-built firmware enabled clustering technology. · The storage model offered should be capable of supporting 3,00,000 or above IOPS and latency equal to or sub 3 mili sec of response time for required IOPS from day one and it should be scalable to 6,00,000 IOPS with scale up/scale out architecture. · Storage should be able to scale 40% more capacity without adding any additional controller. · The storage system should have minimum 384GB 1 TB Global/Federated Data Cache and Expandable upto 768GB 4 TB memory should be delivered on DRAM; any other device or HDD should not be considered as cache.	Please give flexibililty to offer SSD or NVMe SSD if the offered solution is able to meet the required capacity and performance. Higher cache increase the read performance. Every OEM has it's own architecture , some offer global and some federated, if only global is mentioned here then it will become an OEM specific clause.	Global or federated are allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
31	**6**	Disk Drive Support and Encryption	· Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives. - The proposed storage must support data encryption with day 1.	· Offered Storage array shall support various capacities of flash /NVMe flash and NL-SAS drives. Offered storage must support atleast 900 drives considering both SSD and NL-SAS from day 1. · The proposed storage must support data encryption at rest and in flight with day 1.	Since data will be backed. Up to other storage , hence for data security reasons request you to add encyption while data is copied to backup storage.	As per RFP
32	16	Host ports	· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API	~~· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API~~	~~Please clarify what kind of management system will be integrated , this is OEM specific.~~	Since at GFGNL multiple partners and vendors shall utilize the IaaS, To provide the integrity to all of them makes solution generalized
33		Host ports	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, Sub-Lun Data Tiering and other required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity.	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, ~~Sub-Lun Data Tiering~~ and other . The storage must support native method to detect, prevent and restore data in case of ransomware attack. Any hardware/software must be offered from day 1.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	Sub-Lun Data Tiering is optional
34		Host ports	Offered Storage array shall be supplied with at-least dual controllers and 16 x 32 Gbps FC ports across controllers. All offered card shall be capable to work at line speeds.	Offered Storage array shall be supplied with at-least dual controllers and ~~16~~ 32 x 32 Gbps FC ports across controllers and 8 x 25G iSCSI ports.. All offered card shall be capable to work at line speeds.	Please incluse iSCSI ports so that there is flexibility to use both FC and iSCSI ports, also increasing the number of FC ports will help to expand in future and get the required performance.	The bidder can offer better specification as part of the architecture

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
35	19	Remote Replicatio n	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. Any external appliance if needed should be quoted to achieve this functionality.	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. ~~Any external appliance if needed should be quoted to achieve this functionality.~~	This requirement is not for active active replication as. per the RFP specificaiton, if both side will be active then read and write at both ends , hence request you to update this clause. This is favouring one single OEM.	Pls see revision
36		Licenses	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, ransomware protection, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	As per RFP
37		Licenses	`	~~· TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR~~	Pls remove this	Already removed
38		Data Tiering	· Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives.	· Offered Storage array shall be a true flash optimized Hybrid array supporting ~~both SSD NVMe drives and~~ spinning drives.	Since this requiment is for backup , then please explain the role of NVMe SSD's , also if NVMe SSD's are required then it is not mentioned in capacity , it is only asked in NL-SAS drives.	As per RFP

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
39	7	Data Tiering	· Offered Storage array shall be able to tier NVMe SSD and SAS/NL- SAS Drives in a single pool for optimizing performance if required.	· Offered Storage array shall be able to tier NVMe SSD and SAS/NL-SAS Drives in a single pool for optimizing performance if required.	Since capacity is required on NL-SAS drives hence request you to remove this clause	As per RFP
40		Data Tiering	· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API	~~· Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API~~	~~Please clarify what kind of management system will be integrated , this is OEM specific.~~	Repeated query
41		Data Tiering	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, Sub-Lun Data Tiering and other	· The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, ~~Sub-Lun Data Tiering~~ and other . The storage must support native method to detect, prevent and restore data in case of ransomware attack. Any hardware/software must be offered from day 1.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	Repeated Query
42		Data Tiering	required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity.			Question not clear
43	19	Remote Replicatio n	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. Any external appliance if needed should be quoted to achieve this functionality.	· The Proposed storage system should support Active-Active Storage configuration across two sites at Metro distance. ~~Any external appliance if needed should be quoted to achieve this functionality.~~	This requirement is not for active active replication as. per the RFP specificaiton, if both side will be active then read and write at both ends , hence request you to update this clause. This is favouring one single OEM.	Repeated Query

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
44	20	Licenses	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	· Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, , ransomware protection, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.	Ransomware attack are very common these days, since data stored on this storage is critical ,hence request you to add ransomware protection along with the storage.	Repeated Query
45		Licenses	· TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR	~~· TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR~~	Please remove these. Certification	Repeated Query

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
46	57	**SECTION-4 Technical Specification** (4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):) **7 Mobile app**	The mobile app for dashboard/ limited field view with better user experience on handy device is to be provided.	Need more clarity on what exactly is required from Mobile App Dashboard 1. Is the proposed NMS solution required to include a mobile-based site deployment and readiness workflow for managing site rollouts and validations end-to-end? 2. Can the system assign field engineers dynamically based on PoP location, taking into account proximity, workload distribution, and skillset matching? 3. Is there integrated map-based navigation within the mobile app to help field engineers reach deployment sites using GPS routing? 4. Is the proposed mobile application required to support pre-deployment site readiness checks, allowing engineers to upload photos (e.g., electronic components, power availability, cabling) and fill out standardized checklists? 5. Can the mobile app facilitate remote Acceptance Testing Procedures (ATP) by enabling engineers to upload POST photos (e.g., cabling, port connections, LED and POST statuses)? 6. Is the proposed solution required to support capturing and uploading pictorial proof of deployment and	This functionality is essential to increase field deployment efficiency, reduce manual errors, and provide transparency across all stakeholders involved in site rollouts.	Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
				site sign-off, including timestamp and geo-tagging for validation purposes? 7. Is there a centralized, real-time dashboard to track deployment workflows, monitor progress, resolve issues, and perform performance analytics? 8. Is the proposed solution of mobile application and collected data is to be integrate with an existing GIS application, enabling bi-directional feature utilization between the NMS and GIS systems?		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
47	48	**SECTION-4 Technical Specification 4.2** Operational Visibility Platform (NMS + OSS + BSS+ Network visibility): **(Functional Requirements)**	Path computation and optimization	Need more clarity on what exactly is required from Path computation and optimization 1.Does the NMS support integration with SDN controllers for accessing path computation, traffic analysis metrics, topology data, and bandwidth availability? 2.Can the NMS visualize and utilize SDN-derived insights within its dashboard for enhanced network planning and management? 3.Is the solution capable of integrating with at least five SDN controllers from OEMs such as Ciena?	This functionality is not a standard NMS feature and may be required to integrate with SDN controller for smooth network operation and optimization making it essential to amend the RFP compliance accordingly.	Concept is to make NMS ready for the integration with SDN controller such that NMS operator can have the single window access.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
48	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ , Dual Power supply	DDoS vendors provide higher disk capacity in the same DDoS appliance to integrate mitigation, management and reporting into a single device, and these requires use of internal hard drives for storage. However, this type of design comes with certain risks: 1. What happens when the hard drive fails? Should RAID 1 or RAID 5 be used for backup? 2. If the hard drive crashes, even the reports may be lost. These limitations pose certain security concerns. In contrast, Radware DDoS follows a different design philosophy. The DP (DefensePro) deliver high-performance DDoS mitigation. The internal hard drive is only used as a buffer, temporarily holding data before it is transferred to the Cyber Controller for centralized storage—thereby avoiding the above-mentioned risks.	For wider participation internal or external disk is allowed

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					A DDoS must be Stateless technology working on L2 so that it processes traffic packet-by-packet without maintaining connection state, to efficiently handle high volumes of traffic and prevent attacks that exploit stateful devices like firewalls. DDOS device is first in line of defence in network as per best practice in any organization. Organisation should not store any logs related to security events on the hardware which can be accessed by attackers or from outside world. DDoS device is a Stateless device, and it doesn't need to manage connection details resulting in reduction of computational load as per best practice and industry standard. DDoS device does not actively participate in session establishment and does not maintain state of sessions. At most, it passively monitors traffic flows to profile their behavior and to identify certain threats, such as high-rate PPS attacks, network	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					bandwidth floods, etc. Also, it is not recommended to have built-in bypass as per industry best practice.	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
49		4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	DDoS vendors provide higher disk capacity in the same DDoS appliance to integrate mitigation, management and reporting into a single device, and these requires use of internal hard drives for storage. However, this type of design comes with certain risks: 1. What happens when the hard drive fails? Should RAID 1 or RAID 5 be used for backup? 2. If the hard drive crashes, even the reports may be lost. These limitations pose certain security concerns. In contrast, Radware DDoS follows a different design philosophy. The DP (DefensePro) deliver high-performance DDoS mitigation. The internal hard drive is only used as a buffer, temporarily holding data before it is transferred to the Cyber Controller for centralized storage—thereby avoiding the above-mentioned risks.	We have already allowed both the options of stateful and stateless.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					A DDoS must be Stateless technology working on L2 so that it processes traffic packet-by-packet without maintaining connection state, to efficiently handle high volumes of traffic and prevent attacks that exploit stateful devices like firewalls. DDOS device is first in line of defence in network as per best practice in any organization. Organisation should not store any logs related to security events on the hardware which can be accessed by attackers or from outside world. DDoS device is a Stateless device, and it doesn't need to manage connection details resulting in reduction of computational load as per best practice and industry standard. DDoS device does not actively participate in session establishment and does not maintain state of sessions. At most, it passively monitors traffic flows to profile their behavior and to identify certain threats, such as high-rate PPS attacks, network	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					bandwidth floods, etc. Also, it is not recommended to have built-in bypass as per industry best practice.	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
50	59	4.4 DDoS - Distributed Denial-of-Service, Point No. 2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	**Hence requesting you to change this point as below:** should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ , Dual Power supply	DDoS vendors provide higher disk capacity in the same DDoS appliance to integrate mitigation, management and reporting into a single device, and these requires use of internal hard drives for storage. However, this type of design comes with certain risks: 1. What happens when the hard drive fails? Should RAID 1 or RAID 5 be used for backup? 2. If the hard drive crashes, even the reports may be lost. These limitations pose certain security concerns. In contrast, Radware DDoS follows a different design philosophy. The DP (DefensePro) deliver high-performance DDoS mitigation. The internal hard drive is only used as a buffer, temporarily holding data before it is transferred to the Cyber Controller for centralized storage—thereby avoiding the above-mentioned risks.	Repeated query

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					A DDoS must be Stateless technology working on L2 so that it processes traffic packet-by-packet without maintaining connection state, to efficiently handle high volumes of traffic and prevent attacks that exploit stateful devices like firewalls. DDOS device is first in line of defence in network as per best practice in any organization. Organisation should not store any logs related to security events on the hardware which can be accessed by attackers or from outside world. DDoS device is a Stateless device, and it doesn't need to manage connection details resulting in reduction of computational load as per best practice and industry standard. DDoS device does not actively participate in session establishment and does not maintain state of sessions. At most, it passively monitors traffic flows to profile their behavior and to identify certain threats, such as high-rate PPS attacks, network	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					bandwidth floods, etc. Also, it is not recommended to have built-in bypass as per industry best practice.	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
51		4.4 DDoS - Distributed Denial-of-Service	Additional Clause	DDoS technology has to be Stateless appliance so that it can handle an unlimited number of concurrent attack sessions.	DDoS vendors provide higher disk capacity in the same DDoS appliance to integrate mitigation, management and reporting into a single device, and these requires use of internal hard drives for storage. However, this type of design comes with certain risks: 1. What happens when the hard drive fails? Should RAID 1 or RAID 5 be used for backup? 2. If the hard drive crashes, even the reports may be lost. These limitations pose certain security concerns. In contrast, Radware DDoS follows a different design philosophy. The DP (DefensePro) deliver high-performance DDoS mitigation. The internal hard drive is only used as a buffer, temporarily holding data before it is transferred to the Cyber Controller for centralized storage—thereby avoiding the above-mentioned risks.	Repeated Query

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					A DDoS must be Stateless technology working on L2 so that it processes traffic packet-by-packet without maintaining connection state, to efficiently handle high volumes of traffic and prevent attacks that exploit stateful devices like firewalls. DDOS device is first in line of defence in network as per best practice in any organization. Organisation should not store any logs related to security events on the hardware which can be accessed by attackers or from outside world. DDoS device is a Stateless device, and it doesn't need to manage connection details resulting in reduction of computational load as per best practice and industry standard. DDoS device does not actively participate in session establishment and does not maintain state of sessions. At most, it passively monitors traffic flows to profile their behavior and to identify certain threats, such as high-rate PPS attacks, network	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					bandwidth floods, etc. Also, it is not recommended to have built-in bypass as per industry best practice.	

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
52	Page 215 & 34	3.2.1 technical qualification criteria & format XII	In the first criteria, the number of network nodes in WAN are asked but the format XII mentioned about all equipment in the network and also the format is not in line with any of the other criteria.	Request for a change in format XII where the client and the order details of the WAN nodes are asked to comply with the technical evaluation criteria.		Pls see revision
53	Page 133 & Page 194	6.1.14 Existing Infra HOTO & 9.3 Annexure B- Existing S-NOC infra	Bidder shall take the HOTO of existing IT infra like Video wall, computer terminals and Non IT infra like furniture, UPS. AMC of the these infra shall be responsibility of the bidder. Information is given in Annexure B	Please confirm we need to quote for the AMC of these equipment's for 7 years + 3 years. Incase the OEM declares any of its product EOL & EOS then GFGNL will purchase the same without burden to SI please confirm?		Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
54	Licensing	· The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.	· The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR site. · Single license file should be supplied to protect virtual machines/physical servers/NAS workload/Endpoints OR multi cloud workload including all database applications running on these platforms · The proposed backup software should have a native solution to protect Kubernetes/Container workloads; without the need of a 3rd party solution.		Concept is to deploy a single software which can serve the asked requirement. If allow optional, rest of the applications are unserved.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		and DR site. · Single license file should be supplied to protect virtual machines, physical servers, NAS workload, Endpoints and multi cloud workload including all database applications running on these platforms · The proposed backup software should have a native solution to protect Kubernete				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		s/Containe r workloads; without the need of a 3rd party solution.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
55	Reporting Capabilities	· Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve				No clarification asked

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		this functionality. All necessary hardware resources required to run this module should be supplied. . Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts. . Proposed solution				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		should have security and compliance dashboard inbuilt with the product. . Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
56	Security &Compliance	· The backup software must have YARA rules defined in the system. · The proposed solution should have on demand scans available for malware attacks. · The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks. · The	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. YARA is an opensource tool and not meant for Enterprise Solutions. Also, it is Customer responsibility to write the RULEs to filter to out malware infection. There is not quratine available with YARA rules.	· The backup software must have YARA rules/equivalent defined in the system. · The proposed solution should have on demand/scheduled scans available for malware attacks. · The backup Software must have detection & in guest detection via guest indexing against any malware attacks. · The proposed backup software should have MPA approvals for prevention against any backup deletion, accidental or malicious deletion or encryption of backups.		Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		proposed backup software should have four eyes approval for any backup deletion.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
57	Backup support for hypervisors and Applications	· Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention.	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. Instant recovery terminilogy is specific and should use more standard open industry teminilogy.	· Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention. · The proposed backup software should provide Instant recoveries/live mount for any backup to Vmware or Hyper-V Virtual machine. · Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine. · The Proposed Backup Software should support Syslog and Service Now integration or support API. · Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.		Since it's a telecom network environment where fast restoration is high priority, live mount shall not require. However pls refer revision for API support.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		· The proposed backup software should provide Instant recoveries for any backup to Vmware or Hyper-V Virtual machine. It should also support the Instant VM recovery for AHV workloads as well. · Backup software should support file level recovery from any backup of any VM or physical server. It should				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		support a full system recovery in case of a system crash, either on a physical system or virtual machine. · The Proposed Backup Software should support Syslog and Service Now integration. · Backup software should support Multi factor authentication for accessing Backup console and				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		console auto log-off functionality.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
58	RPO/ RTO and Recovery Assurance	· Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability. · Recovery verification should automatically boot the server from backup and verify the recoverability of VM image,	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. The terminilogy "powered-on in a sanbox" is a specific OEM terminilogy, again giving OEM competitive edge and commercial advantage. Hardened the Linux Repository is again an OEM specific terminilogy been used by a specific OEM we request to modify this clause and remove all OEM specific terminilogy. The proposed method for instant file sharing involves mounting NAS files directly from the backup storage, which would essentially be emulated through Object Storage—since Object Storage is a part of the required solution. However, this approach is counterproductive as it relies on the backup servers to mount and serve NAS mount points, placing additional load	· Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox/isolated environment and tested for its recoverability. · Recovery verification should boot the server from backup to verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits. · Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities. · Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks. · Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be		The equivalence is allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits. · Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate	on them. Moreover, this method appears to be tailored to the capabilities of a specific OEM, giving them an unfair advantage in the RFP process. We kindly request that such OEM-specific clauses be removed to ensure a fair, open competition that encourages broader participation and better price discovery.	restored from the backup copies. This will help in complying to "right to be forgotten “regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities. . Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		or ransomware attacks. . Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		"regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
59	Backup and Replication Performance and SLA	· The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads. · Backup software should provide Recovery of Applicatio				No clarification asked

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		n Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO. · The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
60	Disaster Recovery Capabilities	· Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destinatio	A 5-second RPO also implies that the customer has allocated enough bandwidth to make sure data replication happens within that timeframe. AN increase with distance, event a 50-100ms delay can disrupt a 5 - second RPO especially during peak hours or with high-write workloads with overhead of maintaing application consistenency. 5-sec RPO look over ambitious and we request to modify this clause.	· Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site. · The Proposed solution should support Continuous replication at VM level. The RPO must be less than 15 Mins and it must deliver Application consistency. · Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dis- similar systems like hyper converged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. · Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability		Since Back is to take at the same place and Telecom data is highly critical RPO is kept demanding.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		n site. · The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency. · Backup and replication software must deliver maximum investment protection by supporting replication		should be built in for the physical servers and should even work on the dissimilar hardware.		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		of workloads between dis- similar systems like hyper converged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. · Backup software should				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		dissimilar hardware.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
61	Warranty	· 7+3 extendable years 24x7 comprehensive warranty from the server OEM from day one.				No clarification asked

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
62	Licensing	· The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.	· The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR site. · Single license file should be supplied to protect virtual machines/physical servers/NAS workload/Endpoints OR multi cloud workload including all database applications running on these platforms · The proposed backup software should have a native solution to protect Kubernetes/Container workloads; without the need of a 3rd party solution.		Repeated query

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		and DR site. · Single license file should be supplied to protect virtual machines, physical servers, NAS workload, Endpoints and multi cloud workload including all database applications running on these platforms · The proposed backup software should have a native solution to protect Kubernete				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		s/Containe r workloads; without the need of a 3rd party solution.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
63	Security &Compliance	· The backup software must have YARA rules defined in the system. · The proposed solution should have on demand scans available for malware attacks. · The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks. · The	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. YARA is an opensource tool and not meant for Enterprise Solutions. Also, it is Customer responsibility to write the RULEs to filter to out malware infection. There is not quratine available with YARA rules.	· The backup software must have YARA rules/equivalent defined in the system. · The proposed solution should have on demand/scheduled scans available for malware attacks. · The backup Software must have detection & in guest detection via guest indexing against any malware attacks. · The proposed backup software should have MPA approvals for prevention against any backup deletion, accidental or malicious deletion or encryption of backups.		Pls see previous response

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		proposed backup software should have four eyes approval for any backup deletion.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
64	Backup support for hypervisors and Applications	· Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention.	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. Instant recovery terminilogy is specific and should use more standard open industry teminilogy.	· Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention. · The proposed backup software should provide Instant recoveries/live mount for any backup to Vmware or Hyper-V Virtual machine. · Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine. · The Proposed Backup Software should support Syslog and Service Now integration or support API. · Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.		Pls see previous response

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		· The proposed backup software should provide Instant recoveries for any backup to Vmware or Hyper-V Virtual machine. It should also support the Instant VM recovery for AHV workloads as well. · Backup software should support file level recovery from any backup of any VM or physical server. It should				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		support a full system recovery in case of a system crash, either on a physical system or virtual machine. · The Proposed Backup Software should support Syslog and Service Now integration. · Backup software should support Multi factor authentication for accessing Backup console and				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		console auto log-off functionality.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
65	RPO/ RTO and Recovery Assurance	· Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability. · Recovery verification should automatically boot the server from backup and verify the recoverability of VM image,	These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. The terminilogy "powered-on in a sanbox" is a specific OEM terminilogy, again giving OEM competitive edge and commercial advantage. Hardened the Linux Repository is again an OEM specific terminilogy been used by a specific OEM we request to modify this clause and remove all OEM specific terminilogy. The proposed method for instant file sharing involves mounting NAS files directly from the backup storage, which would essentially be emulated through Object Storage—since Object Storage is a part of the required solution. However, this approach is counterproductive as it relies on the backup servers to mount and serve NAS mount points, placing additional load	· Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox/isolated environment and tested for its recoverability. · Recovery verification should boot the server from backup to verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits. · Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities. · Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks. · Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be		Pls see previous response

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits. · Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate	on them. Moreover, this method appears to be tailored to the capabilities of a specific OEM, giving them an unfair advantage in the RFP process. We kindly request that such OEM-specific clauses be removed to ensure a fair, open competition that encourages broader participation and better price discovery.	restored from the backup copies. This will help in complying to "right to be forgotten “regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities. . Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		or ransomware attacks. . Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		"regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
66	Disaster Recovery Capabilities	· Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destinatio	A 5-second RPO also implies that the customer has allocated enough bandwidth to make sure data replication happens within that timeframe. AN increase with distance, event a 50-100ms delay can disrupt a 5 - second RPO especially during peak hours or with high-write workloads with overhead of maintaing application consistenency. 5-sec RPO look over ambitious and we request to modify this clause.	· Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site. · The Proposed solution should support Continuous replication at VM level. The RPO must be less than 15 Mins and it must deliver Application consistency. · Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dis- similar systems like hyper converged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. · Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability		Pls see previous response

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		n site. · The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency. · Backup and replication software must deliver maximum investment protection by supporting replication		should be built in for the physical servers and should even work on the dissimilar hardware.		

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		of workloads between dis- similar systems like hyper converged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. · Backup software should				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		dissimilar hardware.				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
67	26	3.1.1 Eligibility Criteria:	Eligibility Criteria	Kindly allow MSME companies to be part of this bid by means of adding them as a part of consortium to a bidder having 100% eligibility criteria.	We, Tribastion Technologies, are into securing businesses from different threats by different means. NOC is critical operation and needs specilized talent and skillsets to handle such operations. We are a new company and are currently handling critical operations of one of India's top conglomerates. we wish to be part of this RFP however there are no provisons. we humbly requst you to allow companies having valid UDYAM(MSME) certificate to be part of consortium wherein lead bidder has to 100% comply to PQ and consortium partner can join them for a specific work for which they intend to become consortium partner. This will help all such similar companies like us to grow, flourish, use their technical and business acumen to fullfill bid's requirements. This will also show the government's support to small MSMEs by enabling them to bid and be part of such bids which is going to bring disruptions in coonecting India with its roots.	At GFGNL, our primary focus is on enhancing GP connectivity. Concurrently, we are in the process of developing a Network Operations Center (NOC) where the primary tasks will include monitoring and managing the network. We have specified the need for adequate security tools to ensure a robust network infrastructure. However, it is important to note that the consortium's expertise in cybersecurity is not the primary focus of this RFP.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
68	4.1 9/1 /94	Functional ity	End point protection software shall be single agent software for NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates.	**Change clause to below** End point protection software shall be single agent or dual agent from same OEM For NGAV, EDR, Threat Hunting, Application Control, Vulnerability Protection, Firewall, and Device Control, operable without additional updates. Justification by Bidder: As there are multiple functioanlities asked in the Clause hence relaxing the clause from single agent to dualagent from same OEM as suggested will a low maximum participation		For wider participation the double agent is allowed. Pls see revision.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
69	4.3/3/57	Functionality	The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS.	**Change clause to below** The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks,malicious IP addresses, hosts etc. for correlation and blocking in the NIPS **or using endpoint tool ,Bidder can propose integration platform to achieve this functionality** Justification by Bidder: As STIX/TAXII are open platform and blocking may require integration with proposed endopoint solution hence intelligence sharing can happen via endpoint and NIPS integration than it will help to achieve the functionality and allowing broader participation		Pls see Revision for allowing option to achieve desire functionality for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
70	4.3/3/58	Functionality	Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality.	**Change clause to below** Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy or **have it own learning mechanism to understand network traffic pattern to create a baseling for anamoly an to shield vulnerabilities** Justification by Bidder: As NIPS itself have signatures hence integration with third party vulnerbaility scanner is not always required hence changing this clause as suggested will relax the clause and allow broader participitaion thus removing OEM specific functionality		Pls see Revision for allowing option to achieve desire functionality for wider participation
71	58	4.4 DDoS - Distributed Denial-of-Service	(2) Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.	Different OEMs have different ways to fulfil the solution requirement. Requesting 4 TB SSD may limit the participation. Kindly allow bidder to provide memory as per solution requirement.	Should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual power supply & memory as per solution requirement.	For wider participation internal or external disk is allowed
72	58	4.4 DDoS - Distributed Denial-of-Service	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,	Since URLs are encrypted, external URL decryption mechanism is required to install certificate, broker the handshake and decrypt the URL packets. Kindly remove URL from the DDoS solution requirement as it is unfeasible by any DDoS solution technically.	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, blacklist and whitelist,	The equivalence is allowed for wider participation

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
73	72	4.9 Core Router	Core Router, BNG, Carrier Grade NAT, DDoS	Different OEMs have different ways to fulfil the solution requirement. Kindly allow the bidders to quote single or multi-box solutions to achieve the functionalities of Core Router, BNG, Carrier Grade NAT, DDoS for wider participation.	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, DDoS as per RFP.	BNG and Core Router should be in separate box, CGNAT and DDoS can be combine or separate. The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
74	69	4.8 Carrier Grade NAT	(1) Hardware Architecture •The appliance-based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one	CGNAT, AVC, IPS are different functionalities. Every OEM have different ways to meet the solution requirement. Kindly allow bidder to quote single or multibox solution for wider participation.	Bidder is allowed to quote single or mulit-box solution to meet the technial functionality of Core Router, BNG, Carrier Grade NAT, AVC, IPS, DDoS as per RFP.	BNG and Core Router should be in separate box, CGNAT, DDoS and security devices can be combine or separate. The intend of eliminating others is something be discouraged. It is SI responsibility to manage services against high payouts.
75	66	4.7 BNG	(1) General Capabilities The solution should have external NAT capability	This clause is very restrictive in nature as it mandates the NAT capability outside of BNG.	The solution should have NAT capability achieved through same box or multi-box solution.	Pls see revision
76	66	4.7 BNG	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps switching capacity with 2200 Mpps forwarding performance.	Mentioning throughput in Mpps is very specific to and favoring particular OEM, kindly mention throughput requirment in Tbps for wider participation.	(1) General Capabilities The user plane / data plane solution should have minimum 8 Tbps FD switching capacity. All the necessary hardware, software and licenses must be supplied with	Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					the chassis from day-1 with life-time validity of licenses.	
77	66	4.7 BNG	Reliability: • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover)	This is not applicable for BNG with physical deployments in case of PNFs.	Reliability: • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover). Incase of PNF deployment - Any failover procedure in controller card shall preserve the subscribers' sessions (Hitless Failover).	The participation is allowed
78	66	4.7 BNG	Lawful Interception: • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover)	This is not applicable for BNG with physical deployments in case of PNFs.	Lawful Interception: • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover). Incase of PNF deployment - Any failover procedure in controller card shall preserve the subscribers' sessions (Hitless Failover).	The participation is allowed

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
79	69	4.8 Carrier Grade NAT	(5) Management Functions	This architecture is specific to OEM and restricts participation.	Bidder is allowed to meet the technical requirement of management through EMS.	Deemed Optional 1. We are not intending for any proprietary terminologies and elimination of competition merely on ground of proprietary words / monopolized ask, insertion of wrong functional fitment, legacy technology protocols. 2. To address this issue in general, the equivalence of any standard, proprietary words / monopolized ask, bidder / OEM may provide equivalence of the same to avoid disqualification on minor grounds. In case of insertion of wrong functional fitment in broad product segment which is eliminating competition then it is deemed optional. 3.The above is general principle and will apply across the RFP to derisk from propriety terminology and elimination of competition. Hence,

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
						participants may go through the scope of work, functional aspects, supportive technical language for better understanding.
80	72	4.9 Core Router	(7) Temperature & Humidity Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Since the installation is going to be in a temperature controlled Datacenter environment, kindly relax the temperature clause for 5 to 40 degree C	Operate within a temperature range of 5 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing	Pls see revision
81	72	4.9 Core Router	(4) Routing and protocols Segment routing, SR TE, SR PCE, SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	For wider participation	Segment routing, SR TE, SR PCE / SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.	The equivalence is allowed for wider participation
82	74	4.10 Core Switch	•TEC GR 480060:2023	•TEC GR 480060:2023 or equivalent	For wider participation	Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
83	74	4.10 Core Switch	(1) Architecture It shall support 1:1/N+1 redundancy and reliability for critical features such as components power supplies and fans to eliminate single points of failure.	Since modular switch is requested with payload slots for future expansion, the most important and critical reliability aspect of having redundant controller card must be considered. Requesting for high throughput modular chassis without redundant controller card will put critical traffic at stake.	It shall support 1:1/N+1 redundancy and reliability for critical features such as controller cards, power supplies and fans to eliminate single points of failure	Pls see revision
84	75	4.11 Access Switch	•TEC GR 480060:2023	•TEC GR 480060:2023 or equivalent	For wider participation	Pls see revision
85	84	4	Virtualization software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	*The Particular Point is pertaining to Specific OEM and is restrictive in nature*, also this functionality can be achieved via other methodologies, also to Achieve Zero Downtime, Hardware Infrastructure plays a Major Role. *You may ask for 99.95% Uptime of the Proposed Setup that is useful for GFGNL.*	Requested to remove this Point. Or change as per below : Virtualization software should provide 99.95% Uptime with zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	For Wider participation pls see the revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
86	85	17	Virtualization platform shall have FIPS 140-2 Compliance & TLS 1.2 Support as Default Enhanced security compliance	The Particular compliance is pertaining to Specific OEM and is restrictive in nature, also this functionality can be achieved via other methodologies, also to bring to your Notice that FIPS 140-2 is an Encryption Standard which is Specific for US Federal Agencies. kindly refer : https://en.wikipedia.org/wiki/FIPS_140-2 As this Point Restricts other INDIAN OEM's Like us to Participate in the Bid, hence would request you to remove the Point. We do have encryption and support TLS 1.2 and SSL	Requested to remove this Point. Or change as per below : Virtualization platform shall have FIPS 140-2 Compliance or TLS 1.2 Support as Default Enhanced security compliance	For Wider participation pls see the revision
87	85	6	Virtualization management software console shall allow to Move a powered off virtual machine from one physical server to another by dragging and dropping the virtual machine icon.	*The Particular compliance is pertaining to Specific OEM*, also this is a feature which is specific to a Particular OEM and is restrictive in nature. *Also there may not be any particular business function disruption due to Non-Availability of this Specific Feature, hence would urge you to remove this Point.*	Requested to remove this Point.	For Wider participation pls see the revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
88	26	3.1.1 Eligibility Criteria:	-	We request addition of this clause : A bid submitted by a Bidder who has acquired a Company/ Division of a company/100% owned subsidiary company shall also be considered for evaluation if the eligibility and technical evaluation criteria are met jointly by the bidder and the Company/ Division acquired/100% owned subsidiary company.	Justification for the Requested Clause Addition: **Recognition of Business Acquisitions & Continuity**: Companies often acquire other entities or divisions to enhance their capabilities. Allowing such bidders to qualify ensures that expertise, resources, and past experience of the acquired entity are not disregarded. **Fair Evaluation of Capabilities:** If the bidder and the acquired company/division together meet the eligibility and technical evaluation criteria, their combined capabilities should be considered to ensure a fair assessment of the bidder's potential. **Industry Practice & Precedents:** Many tenders allow for the experience and credentials of acquired entities to be counted towards eligibility, ensuring fair competition and allowing experienced market players to participate effectively.	For wider participation, pls see revision.

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
					Encouraging Market Growth & Investment: Supporting acquisitions and business consolidations by recognizing their credentials promotes industry growth, investment, and business continuity.	

==========End Of Document==========

Clarification

Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center for ABP (Phase-III)-GFGNL in Gujarat

Issued by:
Gujarat Fibre Grid Network Limited
GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016/NOC

17th May 2025

Issued By:

Gujarat Fibre Grid Network Limited (GFGNL)

A Government of Gujarat Company

Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Clarifications:

We have observed certain minor level contradictions/typo errors in the RFP and subsequent corrigendum. The following is clarified as corrections for proper bid submissions:

1. The warranty of 5 years is typo-error in SAN Switch and it is contradicting with standard warranty clause. It is clarified that standard warranty clause is applicable on SAN Switch as well.
2. In the last corrigendum related to Next Generation firewall, the threat prevention throughput was changed by mistake i.e. 60 Gbps. The same is reinstate back to 50 Gbps for wider participation.
3. The note mentioned in delivery timeline related to CAMC (Comprehensive Annual Maintenance Contract) is by typo error.
4. CGNAT: Specification/functionality which is not related to CGNAT is deleted for wider participation.
5. Back up storage is mentioned in technical specification at point no 4.16. However, Backup storage was removed by mistake in financial bid. Hence it is reinstate in the financial bid.
6. In lieu of applicable TEC GR certification, for wider participation of multiple products, the bidder may provide compliance of applicable TEC GR.
7. Annexure XII which is related with technical/product credentials and for ease of submissions, the option of authorized signatory with authorization proof is also allowed. In other words ‘CA/CS certificate’ can be read as ‘CA/CS/Authorized signatory’.

==========End Of Document==========

Clarification-II

Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center for ABP (Phase-III)-GFGNL in Gujarat

Issued by:
Gujarat Fibre Grid Network Limited
GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016/NOC

23rd May 2025

Issued By:

Gujarat Fibre Grid Network Limited (GFGNL)

A Government of Gujarat Company

Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Fact sheet:

#	Particular	Details
9	Last date for submission of Bid/proposal	~~04/04/2025,11/04/2025,17/04/2025 at 06:10 pm,~~ ~~28/04/2025~~ ~~08/05/2025~~ -- ~~→22/05/2025 at 6:10 pm~~ →26/05/2025 at 3:10 pm

Clarifications:

We have observed certain minor level contradictions the RFP and subsequent corrigendum. The following is clarified as corrections for proper bid submissions:

1. Technical qualification criteria(new):

   - Point no 1 Bidder capacity → Multiple project **is to be read as** Implementation, Operation and Maintenance of Network Operation Center or State NOC or Data center having network components and managing, monitoring network nodes as part of the project.
   - Point No 8 Presentation→
     a) Previous Project Handling Experience and use cases in unified deployments. (NOC/SOC/Data center, NMS/ Network GIS -3 Marks **to be read as 4 Marks**
     c) Overall Network Performance visibility and management dash board– 3 Marks **to be read as 4 Marks**
     d) Proposed Team size including profile during execution (On site and off site)- 4 Marks **to be read as 6 Marks**
     e) Proposed Team size including profile during O&M (On site and off site (institutional support) (this will be part of contract)- 4 marks **to be read as 6 Marks**

2. Clause no 6.6 Manpower requirement on Payroll of SI (No Subcontracting is allowed) **to be read as follow.** Manpower must be on Payroll of SI for Sr No 1 and 3 (No Subcontracting is allowed). Manpower must be on Payroll or Direct contract of SI for Sr No 2, 4 to 8 (No Subcontracting is allowed). Rest of manpower listed at Sr No 9-12 must be OEM Manpower.
3. Clause 5.41 Delivery timeline → Point no 8 Stabilization and alignment with ABP Phase-III for capex implementation Phase → Payment terms → Remaining 15 % amount shall be paid in 40 equal Quarterly Instalments i.e. 0.375% of CAPEX value per quarter **to be read as** Remaining 15 % amount shall be paid in 12 equal Quarterly Instalments i.e. 1.2 5% of CAPEX value per quarter.

==========End Of Document==========