

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	<p>5.27 - Indemnification</p> <p>5.32 - Patent rights, copy right and IPR</p> <p>The query is responded in Sr no 1197 but probably its taken differently, as visible from the responde.</p> <p>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.</p>	<p>Request for the deletion of 5.32 OR suggested clause - <i>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.</i></p> <p><i>Bidder will facilitate and support GFGNL in the above claims from OEMs</i></p>	<p>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</p>	Pls see revision
5	155	7.7 SLAs for patch managem ent	<p>There are various slabs given for penalty for not meeting 4 categories of patch management (Critical, high.....).</p>	<p>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</p>	<p>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.</p>	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 Integratio n	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 Integratio n	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	<p>Additional points recommended for Fresh NMS and EMS solution</p> <p>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.</p> <p>2]The proposed solution must be Information Security Management System certified with ISO/IEC 27001:2013 and ISO 9001 certificates.</p> <p>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.</p> <p>4] NMS shall be able to capture, track & analyse</p>	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
			<p>traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.</p> <p>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.</p> <p>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</p>			

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

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	<ul style="list-style-type: none"> • infiniband Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter" 	<p>"Please revise this for wider OEM participation as it is restricting us to participate:</p> <p>""• infiniband / Ethernet Options Support for future</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<p>"Please revise as some of terminology is OEM specific:</p> <p>""• 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.</p>	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 /	<p>"• 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."</p>	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	<p>"• infiniband Options Support for future</p> <ul style="list-style-type: none"> • expansions: 100Gb or 200Gb Single or Dual port Adapter" 	<p>"Please revise this for wider OEM participation as it is restricting us to participate:</p> <p>""• infiniband / Ethernet Options Support for future</p> <ul style="list-style-type: none"> • 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	<p>"• 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"</p>	<p>"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"</p>		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	<ul style="list-style-type: none"> • 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." 	<p>"Some of the terminologies are OEM specific please revise as below:</p> <p>""• Server should support agentless management using the out-of-band remote management port.</p> <ul style="list-style-type: none"> • 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 .	Relevant 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 .	Relevant TEC GR for DC level switches.
19	62	4.3 Network Intrusion Prevention System (NIPS)	<p>"• 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.</p> <p>• 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"</p>	<p>"• 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.</p> <p>• The proposed single appliance should deliver 100 60 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 140Gbps on the same box (1 RU) supporting 60M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL having minimal latency."</p>	<p>"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 necessitate the changes</p> <p>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.</p>	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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • All the proposed threat functions support like Full-Stream 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 	<ul style="list-style-type: none"> • All the proposed threat functions support like Full-Stream 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/policy to provide supervision and control. • Should protect against Denial of 	<p>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.</p> <p>SSH inspection causes SSH traffic , breaks the connection and causes issues in regaining connection. There is no specific use case of SSH inspection.</p> <p>Many of the highlighted clauses are OEM specific. Hence kindly modify as per the suggested changes for better participation and with the changes suggested the functional requirement remains same.</p>	Pls see revision

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
			<p>real-time.</p> <ul style="list-style-type: none"> • IPS must deliver more than 10000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities. <ul style="list-style-type: none"> • Firewall Services with Access Lists and time-based Access lists/policy to 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 hidden in 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" 	<p>Service (DOS) and DDOS attacks</p> <ul style="list-style-type: none"> • NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic. <ul style="list-style-type: none"> • 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 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.	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	<ul style="list-style-type: none"> • 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" 	<p>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.</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	117 4	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 functionality of BNG, each subscriber internet traffic on the data plane will land on the BNG, which essentially means if GFGNL plans for accommodating only 100,000 subscribers being served by the BNG with each subscriber 40Mbps Bandwidth, total traffic hitting the BNG by design would be 4Tbps Full duplex. Hence considering scalability and best design practices, BNG should support 8Tbps or more as data plane traffic handling capability	Request GFGNL to maintain data plane bandwidth of 8Tbps 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	<p>Deemed Optional</p> <p>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.</p> <p>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.</p> <p>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</p>	<p>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.</p> <p>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, service automation and automated service provisioning, if a vendor does not support these IETF functionalities in the Core Router, none of the above mentioned services or automation is possible, Core Router at NOC being responsible to aggregate all the Phase I, Phase II and Phase III networks. Hence making this clause optional will put GFGNL in a big issue to comply to other functionalities asked in the RFP.</p>	Request GFGNL to keep all these IETF defined 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 kindly 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 & scalability	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<p>Please give flexibility to offer SSD or NVMe SSD if the offered solution is able to meet the required capacity and performance.</p> <p>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.</p>	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	<ul style="list-style-type: none"> Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives. The proposed storage must support data encryption with day 1. 	<ul style="list-style-type: none"> 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 encryption while data is copied to backup storage.	As per RFP
32	16	Host ports	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 include 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 Replication	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 specification, 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives. 	<ul style="list-style-type: none"> Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives. 	Since this requirement 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	<ul style="list-style-type: none"> Offered Storage array shall be able to tier NVMe SSD and SAS/NL- SAS Drives in a single pool for optimizing performance if required. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, Sub-Lun Data Tiering and other 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity. 			Question not clear
43	19	Remote Replication	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 specifiaiton, 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.	<p>Need more clarity on what exactly is required from Mobile App Dashboard</p> <ol style="list-style-type: none"> 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
				<p>site sign-off, including timestamp and geo-tagging for validation purposes?</p> <p>7. Is there a centralized, real-time dashboard to track deployment workflows, monitor progress, resolve issues, and perform performance analytics?</p> <p>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?</p>		

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	<p>Need more clarity on what exactly is required from Path computation and optimization</p> <p>1.Does the NMS support integration with SDN controllers for accessing path computation, traffic analysis metrics, topology data, and bandwidth availability?</p> <p>2.Can the NMS visualize and utilize SDN-derived insights within its dashboard for enhanced network planning and management?</p> <p>3.Is the solution capable of integrating with at least five SDN controllers from OEMs such as Ciena?</p>	<p>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.</p>	<p>Concept is to make NMS ready for the integration with SDN controller such that NMS operator can have the single window access.</p>

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	<p>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.</p> <p>However, this type of design comes with certain risks:</p> <ol style="list-style-type: none"> 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. <p>These limitations pose certain security concerns.</p> <p>In contrast, Radware DDoS follows a different design philosophy.</p> <p>The DP (DefensePro) deliver high-performance DDoS mitigation.</p> <p>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.</p>	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
					<p>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.</p> <p>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.</p> <p>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</p>	

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

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.	<p>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.</p> <p>However, this type of design comes with certain risks:</p> <ol style="list-style-type: none"> 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. <p>These limitations pose certain security concerns.</p> <p>In contrast, Radware DDoS follows a different design philosophy.</p> <p>The DP (DefensePro) deliver high-performance DDoS mitigation.</p> <p>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.</p>	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
					<p>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.</p> <p>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.</p> <p>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</p>	

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

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	<p>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.</p> <p>However, this type of design comes with certain risks:</p> <ol style="list-style-type: none"> 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. <p>These limitations pose certain security concerns.</p> <p>In contrast, Radware DDoS follows a different design philosophy.</p> <p>The DP (DefensePro) deliver high-performance DDoS mitigation.</p> <p>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.</p>	Repeated query

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

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

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.	<p>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.</p> <p>However, this type of design comes with certain risks:</p> <ol style="list-style-type: none"> 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. <p>These limitations pose certain security concerns.</p> <p>In contrast, Radware DDoS follows a different design philosophy.</p> <p>The DP (DefensePro) deliver high-performance DDoS mitigation.</p> <p>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.</p>	Repeated Query

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

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

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	<ul style="list-style-type: none"> 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 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p>	<ul style="list-style-type: none"> 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. 		<p>Concept is to deploy a single software which can serve the asked requirement. If allow optional, rest of the applications are unserved.</p>

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 Kubernetes				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		s/Contain 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	<ul style="list-style-type: none"> 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
		<p>this functionality. All necessary hardware resources required to run this module should be supplied.</p> <p>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.</p> <p>Proposed solution</p>				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		<p>should have security and compliance dashboard inbuilt with the product.</p> <p>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.</p>				

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
56	Security & Compliance	<ul style="list-style-type: none"> 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 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p> <p>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 quarantine available with YARA rules.</p>	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p> <p>Instant recovery terminology is specific and should use more standard open industry terminology.</p>	<ul style="list-style-type: none"> 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. 		<p>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.</p>

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		<ul style="list-style-type: none"> · 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	RP O/ RT O and Recovery Assurance	<ul style="list-style-type: none"> 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, 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. The terminology "powered-on in a sandbox" is a specific OEM terminology, again giving OEM competitive edge and commercial advantage.</p> <p>Hardened the Linux Repository is again an OEM specific terminology been used by a specific OEM we request to modify this clause and remove all OEM specific terminology.</p> <p>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</p>	<ul style="list-style-type: none"> 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
		<p>Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.</p> <ul style="list-style-type: none"> 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 	<p>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.</p>	<p>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.</p>		

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

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		<p>or ransomware attacks.</p> <p>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"</p>				

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	<ul style="list-style-type: none"> 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 compressi on 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 destination	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, even a 50-100ms delay can disrupt a 5 - second RPO especially during peak hours or with high-write workloads with overhead of maintaining application consistency. 5-sec RPO look over ambitious and we request to modify this clause.	<ul style="list-style-type: none"> 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 dissimilar 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 Backup 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 infrastruct ure to stand alone servers and storage running similar hypervisor s across sites, thereby creating a Disaster recovery environme nt for productio n workloads irrespectiv e 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	Wa rra nty	· 7+3 extendabl e years 24x7 comprehe nsive 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	<ul style="list-style-type: none"> 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 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p>	<ul style="list-style-type: none"> 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/Container 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	<ul style="list-style-type: none"> 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 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p> <p>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 quarantine available with YARA rules.</p>	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value.</p> <p>Instant recovery terminology is specific and should use more standard open industry terminology.</p>	<ul style="list-style-type: none"> 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
		<ul style="list-style-type: none"> · 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	RP O/ RT O and Recovery Assurance	<ul style="list-style-type: none"> 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, 	<p>These proprietary specifications are designed exclusively for one specific OEM, giving them a clear advantage both in terms of competition and commercial value. The terminology "powered-on in a sandbox" is a specific OEM terminology, again giving OEM competitive edge and commercial advantage.</p> <p>Hardened the Linux Repository is again an OEM specific terminology been used by a specific OEM we request to modify this clause and remove all OEM specific terminology.</p> <p>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</p>	<ul style="list-style-type: none"> 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
		<p>Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.</p> <ul style="list-style-type: none"> 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 	<p>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.</p>	<p>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.</p>		

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

SN	PG No	Clause / Sub-clause No	Content of the RFP requiring Clarification	Clarification sought	Justification by Bidder	Response by GFGNL
		<p>or ransomware attacks.</p> <p>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"</p>				

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 destination	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, even a 50-100ms delay can disrupt a 5 - second RPO especially during peak hours or with high-write workloads with overhead of maintaining application consistency. 5-sec RPO look over ambitious and we request to modify this clause.	<ul style="list-style-type: none"> 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 dissimilar 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 infrastruct ure to stand alone servers and storage running similar hypervisor s across sites, thereby creating a Disaster recovery environme nt for productio n workloads irrespectiv e 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.	<p>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 request 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.</p>	<p>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.</p>

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.	<p>Change clause to below</p> <p>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.</p> <p>Justification by Bidder: As there are multiple functionanlities asked in the Clause hence relaxing the clause from single agent to dualagent from same OEM as suggested will a low maximum participation</p>		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	<p>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.</p>	<p>Change clause to below</p> <p>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</p> <p>Justification by Bidder: As STIX/TAXII are open platform and blocking may require integration with proposed endpoint solution hence intelligence sharing can happen via endpoint and NIPS integration than it will help to achieve the functionality and allowing broader participation</p>		<p>Pls see Revision for allowing option to achieve desire functionality for wider participation</p>

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.	<p>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 anomaly to shield vulnerabilities</p> <p>Justification by Bidder: As NIPS itself have signatures hence integration with third party vulnerability scanner is not always required hence changing this clause as suggested will relax the clause and allow broader participation thus removing OEM specific functionality</p>		Pls see Revision for allowing option to achieve desired 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 multi-box solution to meet the technical 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 multi-box solution to meet the technical 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 requirement 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.	<p>Deemed Optional</p> <ol style="list-style-type: none"> 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.	<i>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.</i>	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	<p><u>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</u></p> <p>As this Point Restricts other INDIAN OEM's Like us to Participate in the Bid, hence would request you to remove the Point.</p> <p>We do have encryption and support TLS 1.2 and SSL</p>	<p>Requested to remove this Point. Or change as per below :</p> <p>Virtualization platform shall have FIPS 140-2 Compliance or TLS 1.2 Support as Default Enhanced security compliance</p>	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.	<p><i>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.</i></p> <p><i>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.</i></p>	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:	-	<p>We request addition of this clause :</p> <p>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.</p>	<p>Justification for the Requested Clause Addition:</p> <p>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.</p> <p>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.</p> <p>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.</p>	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=====