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

Dated: 03/03/2025.
GFGNL Ref No: GFGNL/GFG/e-file/263/2025/0016/NOC

Gujarat Fibre Grid Network Limited (GFGNL)
A Government of Gujarat Company
Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar 382010

Contents

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of the Gujarat Fibre Grid Network Limited (GFGNL) or any of their employees or consultants, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

The purpose of this RFP is to provide interested parties with information that may be useful to them in eliciting their financial offers (the "Proposal") pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the TENDERER, in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the TENDERER, its employees or Consultants to consider the investment objectives, financial situation and particular need of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own surveys and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources before filling up the RFP. Any deviation in the specification or proposed solutions will be deemed as incapability of the respective Agency and shall not be considered for final evaluation process.

Information provided in this document to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The TENDERER accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

TENDERER- its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, delay or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way during the Bidding process.

Abbreviations

Sl. No.	Abbreviations	Description
1	BOM	Bill of Material
2	BOOT	Build Own Operate and Transfer
3	DR	Disaster Recovery
4	EMD	Earnest Money Deposit
5	EMS	Enterprise Monitoring System
6	FAT	Final Acceptance Testing
7	ICT	Information and Communication Technology
8	IP	Internet Protocol
9	IPS	Intrusion Prevention System
10	ISO	International Organization for Standardization
11	IT	Information Technology
12	KPI	Key Performance Indicator
13	LAN	Local Area Network
14	LoA	Letter of Award
15	Mbps	Megabit per second
16	MPLS	Multi-Protocol Label Switching
17	MSP	Managed Service Partner
18	NMS	Network Management System
19	S-NOC	Network Operations Centre
20	NSP	Network Service Partner
21	OEM	Original Equipment Manufacturer
22	OFC	Optical Fiber Cable
23	OS	Operating System
24	PAT	Partial Acceptance Testing
25	PBG	Performance Bank Guarantee

Sl. No.	Abbreviations	Description
26	PDC	Primary Data Centre
27	PoP	Point of Presence
28	RFP	Request for Proposal
29	R-S-NOC	Remote – Network Operations Centre
30	SLA	Service Level Agreement
31	SPOC	Single Point of Contact
32	TDS	Tax Deducted at Source
33	TB	Tera Byte
34	UPS	Uninterruptable Power Supply
35	VC	Video Conferencing
36	VLAN	Virtual LAN
37	VoIP	Voice over Internet Protocol
38	VPN	Virtual Private Network
39	VSAT	Very Small Aperture Terminal
40	WAN	Wide Area Network
41	SP	Service Partner

Definitions

Sr. No.	Abbreviation/ Term	Description
1	Acceptance of Letter of award (LoA)	The date on which the successful bidder(s) accepts the letter of award issued by Tenderer.
2	Bidder	The Party who will be offering the solution(s), service(s) and/or materials as required in the RFP. The word Bidder when used in the pre-award period shall be synonymous with party bidding against this RFP
3	Business Hours	The prime utilization period, which shall be starting from 10:30 hrs. till 18:10 hrs. on all working days or as defined by the Tenderer from time to time, unless the specific context requires otherwise.
4	Office Hours	The official working hour of respective offices.
5	Bandwidth Service Partner (BSP)	BSP when used in the RFP denotes the future Bandwidth Service Partner selected by the mode of this RFP.
6	Deliverables	The products, infrastructure, and services to be delivered by the successful bidder in the RFP and Contract, and as proposed in the Proposal and all related documentation/designs/policies and guidelines.
7	End-of-Life	End-of-life is the date of End-of-Sale and/or End-of Support (whichever is earlier) given by the OEM/ on its website or through any public announcement. End-of-Life would be indicating that a product is in the end of its useful lifetime and on the specified dates the vendor will no longer be marketing, selling, or sustaining a particular product and may also be limiting or ending support for the product.
8	End-of-Sale	The date indicated by the OEM/ on its website or through any public announcement, after which the OEM/ stops marketing or selling the product.
9	End-of-Support	Is with reference to a product and is the date indicated by the OEM/distributor on its website or through any public announcement, till which the OEM/distributor will provide service/updates/patches/spare parts/technical support service.
10	FAT	Final Acceptance Testing to test the successful implementation of the scope of work specified in the RFP
11	Fixed Scope	Means the scope of work to be done by the SP as part of the of the RFP.

Sr. No.	Abbreviation/ Term	Description
12	Go-Live	The date of commencement of work and acknowledged by end customer
13	MSP/Managed Service Partner	Managed Services Provider is the company who optimize your communications infrastructure to minimize downtime and remediate problems on your behalf.
14	Original Equipment Manufacturer (OEM)	Manufacturer of any equipment/system/software/product/services who is providing such goods services to the Tenderer's requirement(s).
15	Parties	The Tenderer and the Service Partner collectively, for the purposes of this Contract and "Party" shall be interpreted accordingly to the context therein.
16	Primary Data Centre (PDC)	Primary Data Centre (PDC means a Data Center located at Gandhinagar that would house the Information and Communication Technology (ICT) equipment required for carrying out centralized operations of the BharatNet.
17	Project	The activities to be performed by the Service Partner regarding this RFP
18	Tenderer	Tenderer Means GFGNL or any other government agency
19	Requirements	All the documents prepared by the Tenderer about the Project, Scope of Work, SLA, schedules, details, description(s), statements of technical data, performance characteristics and standards (Indian & International) as applicable and specified in the RFP
20	RFP	The Request for Proposal bearing reference no: ---------- and any other documents/formats provided along with this RFP or issued during the selection of successful bidder(s), corrigenda, seeking a set of solution(s), services(s), materials and/or any combination of them.
21	Service Level	The level of Service and other performance criteria which will apply to the Services delivered by the Service Partner .
22	Service Level Agreement	Service Level Agreement (SLA) is an agreement, to be signed between the successful bidder and the Tenderer includes all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondence, clarifications, presentations for the level of service and other performance criteria which will apply to the services delivered by the Service Partner .

Sr. No.	Abbreviation/ Term	Description
23	Scope of Work/ SoW	To be performed by the Service Partner as provided in RFP and as arising from other clauses of the RFP and includes the requirements and deliverables of the project.
24	Special sites	Special sites are those sites which are to be included for purpose of External Audit. Physical visits for Audit to these sites are necessary. At present there are 70 sites, however, the number may be increased or decreased.
25	Office Hours	Working hours of the GFGNL (10:30 AM to 6:10 PM) on all Working days
26	Day	Day means both working as well as non-working day, unless specified otherwise
27	Customer	Government Offices or any other Enterprise
28	POP	Standard prevailing definition: in the telecom industry (Power backup, connectivity distribution and aggregation, active equipment, Failure protection

STRUCTURE OF THE RFP

Tenderer desires to select **the Agency for Supply, Installation, Commissioning and Operation of Infrastructure and storage of State Network Operation Center -GFGNL.** In this respect, Tenderer is undertaking a comprehensive Tendering process to select the most-suitable Service Partner via competitive Bidding. This RFP is meant to invite proposals from the interested bidders capable of delivering the services described herein. Details of the same are given in following sections:

Section	Description
Section I	KEY INFORMATION & INSTRUCTIONS
Section II	INTRODUCTION
Section III	EVALUATION CRITERIA
Section IV	TECHNICAL SPECIFICATIONS
Section V	INSTRUCTION TO BIDDERS
Section VI	SCOPE OF WORK
Section VII	SERVICE LEVEL AGGREMENT
Section VIII	FINANCIAL BID
Section IX	ANNEXURES & FORMATS

Fact Sheet

The following table provides information regarding the important dates of the bid process:

Sr. No.	Particular	Details
1	RFP Inviting Authority	Gujarat Fibre Grid Network Limited(GFGNL),
2	Job Requirement	**Selection of the Agency for Supply, Installation, Commissioning and Operation of Infrastructure of State Network Operation Center for ABP (Phase-III)-GFGNL in Gujarat**
3	Date of Publication	03/03/2025
4	Availability of RFP Document	The RFP document can be obtained on website Home | GFGNL (gujarat.gov.in) , eProc-Suite (nprocure.com)
5	Name and address for communication, correspondence and seeking clarification regarding the RFP	Chief Finance Officer (CFO) Gujarat Fibre Grid Network Limited (GFGNL), Block No: 6, 5th Floor, Udyog Bhavan, Sector-11, Gandhinagar -382010 dgmnoc-gfgnl@bharatnet.gujarat.gov.in, pmc2@bharatnet.gujarat.gov.in pmc3@bharatnet.gujarat.gov.in, pmc@bharatnet.gujarat.gov.in,
6	Last date for receiving queries/clarifications	The last date of submission of pre-bid queries shall be 12/03/ 2025 at 11: 55.pm All the pre-bid queries should be received on or before the prescribed date and time, through only official email id with subject line as: Pre-bid queries < Bidder's name> The queries should be submitted in an .xls Format as per the format prescribed in RFP document.
7	Time, Date and Venue of Pre-Bid Conference	12/03/2025 at 03:00 pm At Department of Science and Technology, Government of Gujarat/Gujarat Fibre Grid Network

Sr. No.	Particular	Details
		Limited (GFGNL) Block No: 7, 5th Floor, New Sachivalaya, Gandhinagar: 382010
8	Date of response to Bidder Queries	Within 15 days from the date of pre-bid meeting. ***Note:*** *The Tenderer shall not be obligated to respond to any or all the queries. The Tenderer may, at its sole discretion, choose to publish responses to the pre-bid queries and /or any corrigendum on Central Public Procurement portal https://eprocure.gov.in/eprocure/app or may send through email or any other means.*
9	Last date for submission of Bid/proposal	04/04/2025 at 06:10 pm
10	Last date for submission of Bid/proposal (Physical copy excluding financial bid only if asked based on nature of RFP)	06:10 pm (Date of submission of online bid + 4 working Days) In event of particular ask of submitting physical copy then logical portion of the bid should be appropriate in the respective sealed cover for maintaining confidentiality.
11	Bid Processing fee payable	Bidders shall submit, along with their bid, non-refundable bid processing fee of Rs. 15,000/- +GST (Rupees Fifteen Thousand only) in the form of a DD or bank transfer as below: **Details of the Bank:** Bank Name: State Bank of India Bank Account Number: 36242993620 IFSC Code: SBIN0060228 Branch Name: Udyog Bhavan Branch, Gandhinagar Name of the Beneficiary: Gujarat Fibre Grid Network Limited
12	Bid Security/ Earnest Money Deposit (EMD)	**Rs.1,00,00,000/- (Rupees One Crore only)**

Sr. No.	Particular	Details
	Amount Payable	**Details of the Bank:** Name of the Beneficiary: Gujarat Fibre Grid Network Limited Bank details: Bank Name: State Bank of India Bank Account Number: 36242993620 IFSC Code: SBIN0060228 Branch Name: Udyog Bhavan Branch, Gandhinagar
13	Submission of Integrity Pact, EMD, RFP Document Fee and Letter of Authorization	At 06:10 pm (Date of submission of online bid + 4 working Days) for physical copy
14	Address at which bids are to be submitted	Proposal shall be uploaded online in the format and mode as provided for in the Portal ePoc-Suite (nprocure.com) for this RFP in the system and shall be digitally signed by the authorized signatory of the Bidder.
15	Opening of Qualification Bids	To be announced later
16	Opening of Technical Bids	To be announced later
17	Technical Presentation	To be announced later
18	Method of Selection (Define)	QCBS (30:70) H1 based selection
19	Date for the opening of financial bid for technically qualified bidders	To be announced later
20	Contract Duration	7 Year + 3 years extendable
21	Performance Bank Guarantee	5 % of Contract Value

Note: *The above date, time and venue may be altered by GFGNL at its Sole discretion after giving prior notice to the Bidders, some of the information provided in the above Fact sheet is further elaborated in the subsequent sections of this RFP and the information provided in the sections of this RFP are to be read in conjunction and are to be interpreted harmoniously.*

SECTION-1 KEY INFORMATION & INSTRUCTIONS

1.1 Information Regarding RFP

Proposal in the form of the BID is requested for the item(s) in complete accordance with the documents/attachments as per following guidelines.

I. Bidder shall upload their bids on ePROC-Suite (nprocure.com)
II. The Bid Security in the form of EMD in a sealed envelope super scribed with the bid document number to GFGNL office.
III. Bids complete in all respects should be uploaded on or before the BID DUE DATE.
IV. Technical Bids will be opened in the presence of Bidders' representatives who choose to attend on the specified date and time.
V. In the event of the date specified for receipt and opening of bid being declared as a holiday for GFGNL office, the due date for submission of bids and opening of bids will be the next working day at the appointed time.
VI. Services offered should be strictly as per requirements mentioned in this Bid document.
VII. Please spell out any unavoidable deviations, Clause/ Article-wise in your bid under the heading Deviations.
VIII. The bid submitted should be valid for a period of 180 days from the last date of submission of bids**.**
IX. The duration of the Contract period for this activity will be valid for 7 years+ extendable up to 3 years on mutual consent from both the parties.

1.2 Instruction to the bidders for online bid submission

I. Tender documents are available only in electronic format which Bidders can download free of cost from the website https://bharatnet.gujarat.gov.in/ and eProc-Suite (nprocure.com)
II. The bids have been invited through e-tendering route, i.e., the eligibility criteria, technical and financial stages shall be submitted online on the website eProc-Suite (nprocure.com)
III. Bidders who wish to participate in this bid, will have to register oneProc-Suite (nprocure.com), such bidders will have to procure Digital Certificate as per Information Technology Act 2000 using which they can Sign their electronic bids. Bidders can procure the same from (n) code solutions – a division of GNFC Ltd., or any other licensed by Controller of Certifying Authority, Govt. of India. Bidders who already have a valid Digital Certificate need not procure a new Digital Certificate.
IV. Interested and eligible Bidders are required to upload the eligibility related document in eligibility bid section, Technical related document in technical bid section & Commercial Bid in Commercial bid section. The Bids should be accompanied by a bid security (EMD) as specified in this tender document. The Technical & Commercial Bid must be uploaded to eProc-Suite (nprocure.com) &

the Bid Security must be delivered to the office of Gujarat Fibre Grid Network Limited on or before the last date and time of submission of the bid.

V. The eligibility section and the Bid Security section will be opened on the specified date & time in presence of the Bidders or their authorized representative who choose to attend. In the event of the date specified for bid receipt and opening being declared as a holiday for the office of Gujarat Fibre Grid Network Limited the due date for submission and opening of bids will be the following working day at the scheduled times.

SECTION-2 INTRODUCTION

2.1 Introduction

Government of Gujarat (GoG) has implemented BharatNet Phase II Project under "State Led Model". We have set up an SPV namely "Gujarat Fibre Grid Network Ltd (GFGNL)" under Department of Science & Technology (DST) to execute BharatNet Phase -II Project. GFGNL has been created to synergize with the efforts of Government of India under the National Optical Fibre Network and Digital India initiative and make focused efforts to actualize a state-to-village fibre grid and to facilitate building common Government owned infrastructure to provide internet facilities to residents of State of Gujarat.

GFGNL already connected 8,000+ locations mainly comprising Gram Panchayat (GP) along with TC/DC/GIDC/Revenue Villages etc. GFGNL laid around 35,000+ KM of Optical Fiber Cable (OFC), along with active network elements like DWDM technology in core network and GPON technology in access network. The Network Operating Center (S-NOC) has been created in Gandhinagar and it houses all other key network elements like EMS, NMS, GIS, etc. GFGNL also started extending BharatNet connectivity as a Village LAN and Public Wi-Fi from respective GFGNL's Point of Presence (POP)-Gram Panchayats to various offices/Locations of GoG and households.

Carrying vision for developing organization of excellence with distinctive characteristic of building and delivering ultra-speed next generation digital highways serving rural landscape and managing professional partnering ecosystem in urban sphere, for fulfilment of any type of bit transmission requirements of Digital-age government as one-stop digital fabric for all, anywhere and everywhere offices with outer limit of single digit of days commitment by high performing team governed through paperless and faceless new-age systems with high degree of engineering precision and cost effective efficiency.

Project Background:

Phase I:

Under this implementation model, the network infrastructure was deployed by leveraging BSNL's existing Optical Fibre Cable (OFC) from Block to Fibre Point of Interconnect (FPOI) and laying incremental underground OFC from FPOI to GP location.

Number Of Districts	11
Number Of Blocks	117
Number Of GPs	6761

Phase II:

I. The central government had approved a modified strategy to overcome the shortcoming experience during Phase-I project execution and approved the implementation methodology of BharatNet Phase-II to connect remaining Gram Panchayats with state of art network designing with enhance bandwidth to achieve the vision of Digital India.

II. The Government of Gujarat has set up an SPV namely “Gujarat Fibre Grid Network Limited (GFGNL)” to implement Phase-II of BharatNet Project in Gujarat. This SPV has been created to synergize with the efforts of the Government of India under the National Optical Fibre Network and Digital India initiative.

III. These focused efforts are to actualize a state-to-village fibre grid, to facilitate common Government-owned infrastructure, and to provide internet facilities to residents of Gujarat state.

IV. The connectivity is being done by laying end to end (owned) OFC from Block to GPs location.

V. The network architecture was based on linear topology where GPON based electronics infrastructure was deployed across Block and GP location for network mid-haul connectivity.

VI. GFGNL has already connected around 8000 locations mainly comprising Gram Panchayat (GP) along with TC/DC/GIDC/Revenue Villages etc. GFGNL also started extending BharatNet connectivity from respective Gram Panchayat (GP) to various offices/Locations of GoG at the village level.

VII. GFGNL has implemented BharatNet Phase – II network in Gujarat in two different packages. Package – A has three islands in Rest of Gujarat and Package – B has one island in Saurashtra region. Package – A has 12 districts & Package – B has 10 districts. Further, both the packages are divided into two zones. Package A has two zones i.e., Vadodara zone & Surat zone and Package B has two zones i.e., Ahmedabad zone & Rajkot zone.

VIII. Bidders are also requested to get the technical information about the network implemented by GFGNL by referring to the RFP (Request for Proposal (RFP) for Selection of Project Implementing Agency for BharatNet Phase-II project in the State of Gujarat under Gujarat Fibre Grid Network Limited).

IX. GFGNL’s Network comprises of the various technology equipment including GPON, DWDM, OTN, Ethernet, RFMS etc.

X. GFGNL has installed telecom grade shelters and in process of shifting the OLT and other transport devices from BSNL exchange to these shelters. As of now shifting of OLT and other transport devices have already been done in 400 shelters.

Objective of Phase III:

The objectives reflect the project's commitment to providing digital services in equitable manner and contributing to the overall development of the state. The primary objectives of the project are outlined to underscore its strategic goals, which includes:

I. Comprehensive Integration: Seamlessly integrate BharatNet Phase-I and Phase-II networks to establish a unified and cohesive digital infrastructure equitable across the state.

II. Technological Upgrade: Implement IP-MPLS technology for better accessibility/service-offering and ring topology for better network reliability.

III. Expanded Connectivity: Reaching approximately 4400 more villages over and above the existing rural connectivity, to cover full landscape of Gujarat and a step towards everyone’s right to take part in digital journey.

IV. Network scalability: Future traffic demand to be supported with network scalability considered with 1G to 10G at GP level and 10G to 100G at Block Level.

V. Ensuring better customer service: Single S-NOC for the entire network along with 24 x 7 helpdesk support to ensure quality service delivery.

VI. Ensuring operational efficiency: High network availability to be maintained up to 99% by additional OFC to be laid with 24F/48F Armored cable, UPS deployment with minimum 6 Hrs. backup at each GP

VII. Socio-Economic Empowerment: Facilitate digital empowerment by enabling access to education, healthcare, e-governance, and economic opportunities in rural areas. Deployment of mini-OLT at every two GPs with target of approx. 6 lakhs customer over BharatNet network.

VIII. Stakeholder Collaboration: Foster collaboration among GFGNL, the Government of Gujarat, Department of Telecommunication (DOT) and other stakeholders to ensure seamless execution and alignment with national broadband connectivity goals.

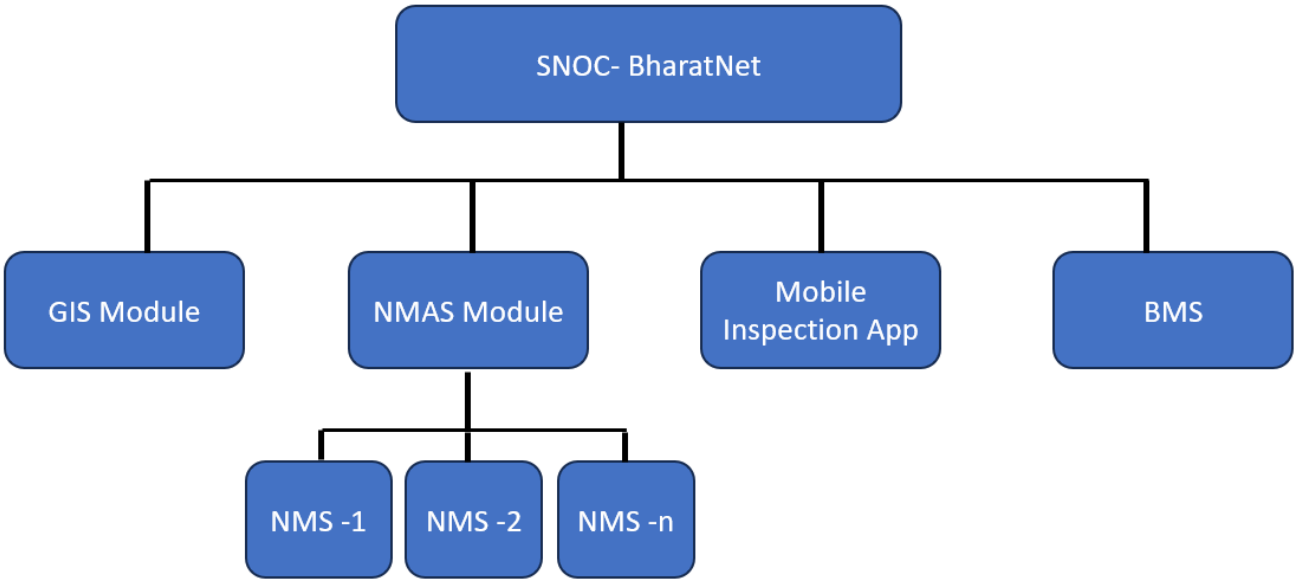
IX. Device types and count are as below but not limited to:

Table 2: Network Element (Indicative):

Sr. No	Device Type	Count
1	DWDM Node	945
2	GP router	15000
3	Mini OLT/switch at GP	14000
4	Block/District Router	1000
5	S-NOC/Core	20
6	RFMS	660
7	CPE Router/switch/ONT	70000
	Total	**101625**

To Fulfill above objective, GFGNL seeking agency to provide core infrastructure as mentioned in Financial bid format. To cater the upcoming requirement of phase III, which will integrate Phase I also, so SI shall come up with the state of the art and cost effective solution.

Logical Diagram:



SECTION-3 EVALUATION CRITERIA

3.1 Qualification Criteria

In the event of disqualification, GFGNL shall be entitled to blacklist the Bidder from participation in the tendering process for GoG/DST/GFGNL the work of Ministry of Communications / Department of Telecom / any public sector undertaking engaged in Telecom and any work under other state Sponsored Schemes for a period of one year from the Bid Date and/or forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated loss and damage likely to be suffered and incurred by GFGNL and not by way of penalty for, inter alia, the time, cost and effort of GFGNL, including consideration of such Bidder's proposal (the "Damages") without prejudice to any other right or remedy that may be available to GFGNL under the Bidding Documents or otherwise. Without limiting the generality of the above, a Bidder shall be deemed to have a Conflict of Interest affecting the Bidding Process, if:

- A constituent of the GFGNL Phase III (ABD- Amended Bharatnet Program) RFP or
- Such Bidder has the same authorized representative for purposes of this Bid as any other Bidder for the same Package or
- For the same Package of GFGNL PH-III RFP, such Bidder, or any Associate thereof has participated as a consultant to GFGNL in the preparation of any documents, design or technical specifications of the Package.

3.1.1 Eligibility Criteria:

Sr. No	Eligibility Criteria	Document Required
1	The Bidder should be an Indian firm – a) Should be registered under the Companies Act 1956 or 2013 in India or a Proprietorship or partnership or an agency should be a firm/LLP at the time of the bidding b) Should have a registered number of, GST, Income Tax / Pan number c) Should be in operation in India for a period of at least 5 years as on publication of this RFP	The Bidder should submit below documents – a) Copy of certification of incorporation issued by competent authority / registration Certificate/ Shop& Establishment certificate. b) Copy of PAN card c) Copy of GST registration
2	The bidder should have average annual turnover of minimum INR 100 Crores from ICT System Deployment (S-NOC/Data center) and technical operations, Software product deployment (S-NOC/NMS software and GIS) and Integration in any three financial years out of last four Financial Year as on 31st March 2024.	The Bidder should submit below document - a) CA certified and audited Balance Sheet and Profit & Loss statement for the three financial years considered till

Sr. No	Eligibility Criteria	Document Required
		March 2024 to meet the requirement as per clause. b) CA certificate mentioning turnover from the said business in financial years considered till March 2024 to meet the requirement as per clause.
3	The bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2024.	The copies of CA Certified Statement for last three financial years as on 31st March 2024 shall be attached along with the bid.
4	The bidder should have experience in successful execution of similar projects for central government or any state government or PSUs or telecom or BFSI or public listed company in India during past five years from the date of bid submission of value specified herein: a) One project with the value of at least 40 crores with 5K network Nodes or b) Two projects, each with the value of at least 30 crores with 4K network Nodes or c) Three projects, each with the value of at least 20 crores with 3K network Nodes Similar Project is defined as: Implementation, Operation & Maintenance of Network Operation Centre or State NOC or Data Centre having (compute, storage, Security and Networking components) and managing, monitoring network nodes as a part of the Project.	Copies of Purchase Order, completion/ Go-live certificate or partial completion certificate complying to the clause requirement from client to be enclosed along with Technical Bid.
5	OEM products: All the OEM products including software components must have proven deployment and commissioning with 5 clients in this RFP in past 7 years. For similar project please refer the definition mentioned above .	OEM Declaration on their letterhead along with work order and proof of successful installation (i.e., Delivery challan or Client certificate on successful installation or OEM certificate from Company Secretary/Legal).

Sr. No	Eligibility Criteria	Document Required
		OEM can mask sensitive information.
6	a) The bidder should be authorized by OEMs of the proposed Product to quote their product or any third-party product to complete the solution as per RFP. b) The bidder should also have a back-to-back support agreement/arrangement with OEMs for after sale support & services including supply of spare parts etc. The proposed product quoted in the bid should not be declared EOL or EOSS for next 7 Years from the date of Bid Submission.	The Bidder should submit MAFs issued by OEMs of the proposed Products with declaration as per clause.
7	The bidder should: a) Not have been banned / blacklisted by Central Government / Any State Government / PSU in India as on the date of bid submission. b) Not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons. c) Not have their directors and officers convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified.	The bidder should submit Self-declaration letter duly signed and stamped by the authorized signatory as per format (format-VII).
8	The Bidder should have at least one office in Gujarat which can provide 24x7 technical support & service to meet SLA	The copy of Property tax bill/Electricity Bill/Telephone Bill /GST /CST, etc. should be enclosed. In case Bidder the is having not any office in then Gujarat, should bidder submit a letter of to open undertaking the office in Gujarat within 45 days from the date of award.
9	The Bidder must possess any three of the following certifications as on date of bid submission -	The Bidder should submit valid certificate.

Sr. No	Eligibility Criteria	Document Required
	a) ISO 9001:2015 b) ISO/IEC 20000-1:2018 c) ISO/IEC 27001:2022 d) CMM -L3 or above	
10	Any Bidder or OEM from a country which shares a land border with India will be eligible to bid in this tender only if bidder is registered with Competent Authority. The Competent authority for the purpose of registration shall be the Registration Committee constituted by the Department of Promotion of Internal Trade (DPIIT) of Govt. of India	The bidder should submit Undertaking with respect to Compliance of Restrictions for Countries which share land border with India – as stipulated by Govt. of India.

Note:

i. Bidders who have submitted the valid EMD and other eligibility documents shall be considered for further evaluation. If bidders fail to submit the bid security other eligibility documents as per this RFP document, the Bid shall be out rightly rejected.

ii. The Bidder must attach valid documents in support to their capabilities/strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable to be rejected.

iii. Technical evaluation will be done only for those bidders who have been found to be in compliance with the Eligibility criteria. The Technical Evaluation Committee based on technical evaluation framework mentioned shall evaluate each proposal and allot technical score as per the technical criteria.

iv. All details and the supportive documents for the above should be uploaded online on tender Portal.

v. A board resolution OR power of attorney in the name of the person executing the bid, authorizing the signatory to commit the Bidder.

vi. All certificates requested in the RFP should be valid as on date of bid submission

vii. All annexures as sought in this bid should be complete as per the information requested.

3.2 Methodology of Selection

BID EVALUATION PROCESS

The TENDERER will form a committee, which will evaluate the proposals submitted by the bidders for a detailed scrutiny. The evaluation will be based on QCBS (30:70) i.e., 30% weightage will be given to technical score and 70% weightage will be given to financial. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarification

of their Proposals.

a. Pre-Qualification evaluation:

I. Bidders who have submitted the valid EMD and other eligibility documents shall be considered for further evaluation. If bidders fail to submit the bid security other eligibility documents as per this RFP document, the Bid shall be out rightly rejected.

II. If there is any lack of clarity in the submitted eligibility documents, evaluation committee may ask additional clarification/ documents from the concerned bidder. Committee may consider the additional documents/ clarifications for evaluation if they are as per the requirement stated in RFP.

III. Upon verification, evaluation/assessment, if in case any information furnished by the Bidder is found to be false / incorrect, their bid will be summarily rejected and no correspondence on the same shall be entertained.

IV. Submission of false/forged documents will lead to forfeiture of EMD and blacklisting of agency for a minimum period of 3 years from participating in Gujarat Govt. tenders.

b. Technical Bid Evaluation:

Technical evaluation will be done only for those bidders who have been found to be in compliance with the Eligibility criteria. The Technical Evaluation Committee based on technical evaluation framework mentioned shall evaluate each proposal and allot technical score as per the technical criteria mentioned below:

3.2.1 Technical qualification criteria

Sr. No	Criteria	Supporting Documents	Max. Marks
1	The bidder should have supplied, implemented and managed following projects in past 5 years. a) NOC (Network Operation Center)- 3 Marks b) Data center- 3 Marks c) NOC, Data center, (NMS/OSS or Network GIS)- 9 Marks Note: • The highest experience based will be given highest marks and there after rest will be given marks on percentile basis.	Copy of Purchase Order/ Work Order/ Agreement/ client certificate	15
2	Demonstration of prototype/readiness to meet technology led Governance in GIS a) Project management- b) Digital measurement book c) Virtual inspection	POC	20

Sr. No	Criteria	Supporting Documents	Max. Marks
	d) The solutions of OEM must provide at least one reference case demonstrating GIS led support for more than 20,000 KM fiberization in any Government, PSU, pubic listed company or Telco- 5 Marks		
3	Demonstration of prototype/readiness to meet technology led Governance in NMS and OSS a) Service provisioning automation level b) Network scanning and KPIs c) Digital SLA measurement d) Dashboard for MD, HQ, District, Client e) High performance architecture for speedier reports and real time calculations. f) Integration convenience/understanding as per telco practice by API/NE of all type of elements in BharatNet. g) Any other important functionality to be shown. h) The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 network elements in any Government, PSU, Bank/ pubic listed company or large-scale IP network- 5 Marks	POC	20
4	Visualization/orchestration in setting up and management for S-NOC (Private -on premise Cloud)	POC	5
5	BSS: a) UX (User Experience), Navigation, ordering and service creation. -2 Marks b) Integration of BSS with OSS in NMS- 2 Marks c) Optimization of licenses in BSS to meet current requirements and future scalability with reduce licensing cost. - 3 Marks d) The solutions of OEM must provide at least one reference case demonstrating support for more than 50,000 Customers in any Government, PSU, Bank/ pubic listed company or large-scale IP network. Presentation to be done for Education department live connections- 3 Marks	POC	10

Sr. No	Criteria	Supporting Documents	Max. Marks
6	Technical and integration architecture, intelligent sizing: a) All ICT infra components, database sizing in consonance with NMS, GIS and BSS. (The best optimized sizing will be given highest score and remaining in proportionate). - 6 Marks b) Outcome of all the above components including integration and software scalability. - 4 Marks	Commitment document	10
7	Presentation: - a) Previous Project Handling Experience in high performance unified deployments. (NOC, Data center, NMS, Network GIS) b) Industry deployment use cases in quoted software products. c) Performance visibility – ICT and service and high availability commitment. d) Technology led governance, data driven supervision, virtual inspection and management dashboard. e) Proposed Team size during execution (On site and off site) including minimum profile in our project (this will be part of contract). * f) Proposed Team size during professional O&M (On site and off site (institutional support)) including minimum profile in our project (this will be part of contract). * * Note: The best proposal in terms of size and profile will be given highest marks and there after rest will be given marks on percentile basis	Presentation PPT	20
	Value added offering over and above the ask of RFP without any additional charges. • Use of Licenses, higher capacity in storage/ No of cores, manpower, contract duration, offering of AI and etc.		10
		Total	100

Note:

i. The Bidder shall submit committal documents to comply with the technical evaluation criteria.

ii. Technical evaluation shall include the evaluation of all the documents mentioned in the Technical Bid. Technical bids shall be examined by the bid evaluation committee with respect to compliance, completeness and suitability of the proposal to the project and only the bids

which are complying to the requirements mentioned in the RFP shall be considered as technically qualified.

iii. The Bidder should obtain minimum 70% score to technically qualify. The financial bids of only technically qualified bidders would be opened.

3.3 Final Bid Evaluation:

3.3.1 Technical Bid Evaluation:

The technical score of a bidder 'Tb' will be assigned to the bidder and it will be awarded based on the Technical Evaluation Criteria as specified above. TENDERER's decision in this regard shall be final & binding and no further discussion will be held with the bidders.

Tb: Absolute Technical Score Tmax: Maximum Technical Score

Tn: Normalized technical score of the bidder under Consideration Normalized technical score (Tn) = Tb/Tmax * 100

3.3.2 Financial Bid evaluation:

The Financial Bids will be opened, in the presence of Bidders' representatives who choose to attend the Financial Bid opening on date and time to be communicated to all the technically qualified Bidders. The Bidder's representatives who are present shall sign a register evidencing their attendance. The name of bidder & bid prices will be announced at the meeting. The financial score of a bidder 'Fb' will be assigned to the bidder.

'Fb' will be the total financial quote made by the bidder

Fn: normalized financial score for the bidder under consideration Fb: commercial quote for the bidder under consideration

Fmin: commercial quote of the lowest evaluated financial proposal

The lowest evaluated Financial Proposal (Fmin) will be given the maximum financial score (Fn) of 100 points. The financial scores (Fn) of the other Financial Proposals will be calculated as per the formula for determining the financial scores given below:

Normalized Financial Score (Fn) = 100 x Fmin / Fb

3.3.3 Final Evaluation of Bid

Proposals will be ranked according to their combined technical (Tn) and financial (Fn) scores using the weights (T = 0.6 the weight given to the Technical Proposal; P = 0.4 the weight given to the Financial Proposal; T + P = 1). The final evaluation will be based on Final Score which shall be calculated as shown below:

Final Score (S) = Tn x T + Fn x P

The bidder achieving the highest combined technical and financial score will be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest combined technical and financial score, the bidder with the higher normalized technical score will be invited first for negotiations for awarding the contract.

Note:

i. Financial Bids that are not as per the format provided in the RFP shall be liable for rejection.

ii. The Bidder must attach valid documents in support to their Technical and Financial capabilities /strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable for rejection.

SECTION-4 Technical Specification

4.1 Geographical Information System (GIS):

Sr. No	Category	Requirement
1	Deployment	• The solution must be a GIS-based web and native mobile application (Android 13.0+ and iOS 15+). All modules must include web and mobile apps except for the Fiber Planning tool, which is web-based only. • The application must support deployment on-premises or in a secure cloud (public/private) environment accessible by users. • Support operation across disparate offices with centralized data storage and database updates synchronized without requiring high-speed network links. • Use open-source databases like PostgreSQL. • Allow importing network data in various formats (Excel, ESRI Shape file SHP, DXF, CSV, Google KML/KMZ, MapInfo Tab). • Enable exporting network data in formats like ESRI Shape file SHP, DXF, XML, CSV, PDF, Google KML/KMZ, MapInfo Tab.

2	PM Tool	• The project monitoring tool shall enable real-time tracking of project progress, (timelines and milestones) including the status of network infrastructure deployment, equipment installation, and connectivity establishment across all packages of Amended BharatNet program.
		• The PIA of GFGNL ABP RFP shall provide the input for managing project documents, drawings, specifications, permits, contracts, and other relevant documentation etc.
		• The PIA of GFGNL ABP RFP shall provide all required information for the application dashboard in standard/ defined format such as measurement book, acceptance test proofs etc. The details shall be, but not restricted to, as under: -
		  ◦ Block/GP wise Cable Length.
		  ◦ Block /GP wise Duct length.
		  ◦ Block /GP wise Trench Length.
		  ◦ Total as build OSP network elements count/details of FDMS/ Hand hole/ Manhole/ Site/ Splice Closure etc.
		  ◦ Total Planned OSP network elements count/details of FDMS/ Hand hole/ Manhole/ Router/ Site/Splice Closure etc.
		  ◦ Total ISP network Elements count/details of Router/ Switch/OLT /Repeater /Equipment's etc.
		• The PIA of GFGNL ABP RFP shall be responsible to update the project progress in the project monitoring tool, enabling the system to automatically create milestone-based proforma invoices.

Sr. No	Category	Requirement
3	API Integration	• Provide REST/SOAP/XML-based integration with OSS, BSS, ERP, and Fiber Management applications. • Modules must support integration with ticketing systems, RFMS for fault locations, NMS/OSS for ISP updates, and GIS-based inventory systems. • Enable integration with SMS, email, and WhatsApp gateways for communication with field technicians/customers.
4	User Management	• The solution shall support single sign-on or authenticate via Active Directory where database is to be provided by PIA of PH-III and implementation to be done by bidder. • The solution must support a 2-way authentication mechanism to access the application by authorized users. • Administrators should be able to create, edit, and delete users, groups, and roles. Users should be assigned roles with varying privileges. • Administrators should be able to assign users to specific modules • The system should enable the creation, editing, and deletion of network entities based on user permissions. • Implement area-based rights, restricting users to view or edit data within their assigned districts/states/blocks/regions. • Support the creation of groups/teams, user log monitoring, and visibility of active users in various groups and roles. • Administrators should be able to restrict users to their locations. Geofencing support is required based on multiple segments such as country, region, and province. • The solution must manage thousands of named users seamlessly. • Support multiple levels of hierarchy and approval mechanisms for created or updated data. • Allow administrators to manage both internal and external users of GFGNL. • Provide specific module access to PIAs along with specific circles, enabling them to manage users as per the defined rules.
5	Base Map & Mapping Platform	• The solution must bundle GIS layers for block boundaries, GP, and village locations. Additional necessary layers for network planning should also be provided. • Users should be able to query block boundaries, GPs, or villages in a district/state. • The solution should use a cloud-hosted map platform like Google Maps, supporting high-resolution satellite imagery, terrain view, and Streetview (where available).

Sr. No	Category	Requirement
		• The base map should include predefined yet customizable administrative features such as boundaries, street centerlines, railways, and waterways. • Support user-configurable layers for custom land base management. • Load/display vector/raster maps, network, and customer data for a given location without relying on Web Mapping Service (WMS). • Support adding and displaying third-party WMS layers. • Ensure consistency in map appearance and symbols across all web and mobile applications. • Administrators should be able to choose attributes of network entities as labels to display over the base map. • Include a Layer Manager functionality for toggling the visibility of layers. • Provide tools to measure distances between points. • Allow users to search for locations, places, and network elements on the map. • Enable advanced filtering to display network data on the map. • Support external map data views (e.g., KML/KMZ, SHP, TAB formats) without adding data to the database. • Provide advanced filtering for project and vendor codes to differentiate and visualize network data on the map. • Allow probing information shown on the base map at multiple zoom scales for detailed insights.
6	Configuration Capabilities	• Administrators should be able to attach forms or checklists, setting mandatory fields as part of the workflow or network process. • Enable adding custom-defined network equipment vendors and specifications, which can be mapped across all inventory entities. • Equipment modeling must be independent of network type or vendor, supporting multi-technology models such as FTTx, GPON/xGPON, xDSL, OTDR, WDM, etc. • All network element data models should use template-based modeling for configurable design specifications. • Assign unique names/IDs to network elements following admin-defined naming rules, with the ability to generate labeled outputs displayed on the map. • Provide an interface for admins to set threshold values for raising alerts on cable and equipment utilization. • Maintain personalized user workspaces to allow users to return to the same working area after session logout.

Sr. No	Category	Requirement
7	Fiber Inventory Management	• Support desktop planning with fiber network design topology, including ring-based and linear-based structures with shortest route determination. • Enable manual and automated creation of child rings if the planned ring exceeds permissible fiber length. • Provide options for various cable configurations (e.g., 24F, 48F, 96F, 144F) and infrastructure elements like ducts, trenches, poles, and routers. • Facilitate connectivity and splicing between cables, equipment, and components at block and GP levels. • Support standard loss configurations for multiple wavelengths (1310 nm, 1550 nm) and optical power loss calculations for endpoints like Gram Panchayats. • Incorporate restricted area planning, allowing users to designate restricted zones on the GIS base map and propose alternative network plans. • Enable planning for both Inside Plant (ISP) and Outside Plant (OSP) networks with integrated geolocation data. • Provide comprehensive land base datasets, including state, district, block boundaries, road networks, and population data for planning purposes. • Support exporting network plans in KML, Shape, and PDF formats with street view features. • Generate detailed reports such as BOM/BOQ, capacity utilization, optical link budgets, and tracing reports in graphical and tabular formats.
8	OSP & ISP Inventory	• Support design and management of fiber networks, including Backbone, Last mile. • Allow placement of infrastructure elements such as ducts, cables, chambers, poles, splices, routers, and ONTs. • Provide tools for civil structure placement (e.g., poles, manholes, ducts) using standard editing tools. • Support various network methodologies, including underground, overhead, and wall-clamped approaches. • Represent Passive and Active elements spatially and attribute-wise, including depth, height, and rack location. • Provide intuitive GUI representation of OSP and ISP components, enabling telecom planning, building, and operation across multi-vendor and multi-technology environments.

Sr. No	Category	Requirement
		• Include a “clone” function for creating new network elements based on existing templates. • Allow bulk import of network elements in formats such as KML, CSV, and Excel, using predefined templates. • Display the construction status of network elements (e.g., in-service, planned, dormant) in the layer manager. • Store audit logs of user updates with username and timestamp. • Support map and non-map editing functions (e.g., move, delete, change attributes) while ensuring data integrity. • Include an approval process for field changes via mobile application. • Manage network stages (planned, as-built, dormant) with bulk transition capabilities. • Visualize fiber states (connected, free, dark, reserved) and manage fiber cores in cables. • Create multiple plans and tag entities with unique project codes for tracking. • Support Inside Plant (ISP) views, including management of rooms, racks, and rack dimensions. • Automatically create network equipment inside racks based on input from NMS/EMS systems via APIs. • Provide graphical views of buildings, floors, risers, and cable connections, including vertical and grounding plans.
9	Optical Power & Loss Calculation	• Enable optical power link budget calculations between reference points, considering user-configurable loss values. • Manage standard attenuation values for splicing, patching, fiber loss, equipment loss, and connector loss at various wavelengths. • Fetch real-time loss details from NMS/EMS systems for cables and equipment via API integrations.
10	Network Modelling & View	• Provide a Network Entity Library with built-in data models for elements like sites, equipment, ducts, cables, manholes, splice closures, and poles. • Offer schematic views of network nodes, such as cables and splice closures, to display connected and free ports. • Allow users to edit locations and attributes of network elements and attach images/documents to any entity. • Manage historical changes on network entities, including attribute and geometrical modifications, with date/time stamping and modifier information.

Sr. No	Category	Requirement
		• Provide graphical and map-based views of end-to-end connectivity across multiple transport mediums. • Manage physical circuits end-to-end, tracing fiber connections from any point bidirectional on the map. • Enable splicing and patching functionalities for cables and equipment, offering traceability of connections upstream and downstream. • Provide splice and patch records (e.g., diagrams, charts) in textual and graphical formats, downloadable as PDFs or Excel files. • Generate shortest paths and alternative routes using road network data, incorporating fiber cut locations from OTDR/Remote Monitoring systems. • Allow optical length input from OTDR devices to determine and plot precise fault locations on the map.
11	Logical View	• Support logical views of equipment at the port level, displaying service information in a single diagram. • Enable service mapping for user-configurable services or services received from NMS/EMS systems, displaying service paths along physical network routes.
12	Automation & Monitoring	• Support bulk updates of network element attributes, like construction stage and location, using CSV templates. • Include an Auto Planning feature for Point-to-Point Backbone Fiber Planning with optimized route generation and BOM/BOQ creation. • Automatically place manholes, hand holes, or poles at equal intervals along planned cable routes. • Monitor the passive utilization of network elements like cables and equipment, triggering auto-notifications/alarms for over utilized components. • Fetch real-time utilization details of active equipment from NMS/EMS systems via APIs, displaying over utilized nodes on the GIS map.
13	Reports	• Generate capacity utilization reports for various network elements. • Provide schematic analysis reports for fiber trace, strand status, circuit design, and facility status. • Allow asset reporting with boundary-based filtering (e.g., administrative or ad hoc). • Support generating standard reports like network entity logs, management, and utilization summaries. • Estimate network elements and cable length within selected regions for auditing purposes.

Sr. No	Category	Requirement
		• Generate HLD and LLD reports for OSP and ISP designs, including geolocation data for elements like FATs, FDTs, and joint enclosures. • Provide complete printing and plotting capabilities, allowing maps and schematic drawings in various paper formats (A0 to A4) and scales (1:500, 1:1000). • Include standard reports and queries accessible in real-time or batch mode via menu selection. • Support scheduling and subscription of reports for automated generation and distribution. • Customize dashboard to be prepared as per the requirement of GFGNL
14	Fiber Inventory Mobile App	• Support network data creation and inventory updates from the field using the mobile app. • Include voice-based network creation features for point objects (e.g., “Create an OLT” command). • Automatically create cables, ducts, and trenches based on the path followed by surveyors. • Display network layers on a map and attach images/documents with geolocation and timestamps. • Provide offline functionality for data capture in remote areas, with synchronization when internet connectivity is restored. • Enable splicing features for Cable-to-Cable, Cable-to-Equipment, and Equipment-to-Equipment connections. • Include cable merge and split features and support network entity grouping and placement. • Allow field users to create work orders, update the network, and submit work orders for managerial approval. • Provide a land base survey module for capturing building data and tagging attributes like name, address, and category (Residential/Commercial).
15	Video Application	• Support video logging for activities like trenching, fiber laying, splicing, and ducting, with GPS coordinates and timestamps. • Record specific details such as trench depth, OFC blowing processes, splicing loss, and water permeability tests, with calibrated measurement tools. • Enable recording of route marker details and generate videos with file descriptions based on predefined nomenclature. • Integrate with DGPS devices for greater accuracy in video surveys.

Sr. No	Category	Requirement
		• Provide concurrent viewing windows on the web application for physical work, activity location on Google Maps, and metadata (e.g., OFC route and depth). • The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases. The scope of the bidder includes ensuring that all video applications forms/function with length and timestamp as intended for various objective. Additionally, the bidder must support all necessary requirements for creating a digitized video/photo geotagging tool, forms in web and mobile as and when required or executed by GFGNL and bidder has to support to define SOP with PIA of Phase 3.
16	Field Operation Management	• Support lifecycle management of work orders, including assignment, escalation, approval matrices, and fault tracking. • Track work order activities such as fiber cuts, Active and passive installations and failures, with photo and geo-tagging features. • Suggest the shortest route to fault or issue locations using GPS. • Enable work order reassignment and manual mapping of related ticket correlations. • Assign work orders based on priority, SLAs, due dates, required skills, dependencies, and location proximity to resources. • Manage field force schedules, including appointments and resource availability. • Assign predefined route maps for scheduled maintenance or patrolling services. • Display patrollers' statuses (e.g., unassigned, in-progress, paused) and track field resources in real-time on the map, including driving speed and battery status. • Manager assigns route to Patroller based on roster: one-time/daily/weekly/monthly. • Includes Patroller Name, Planned Route Start/End Times, Actual Route Start/End Times. • Compare planned vs actual path on map, display distance travelled. • Patroller self-check-in capability, Manager approval or denial. • Supervisor web App for leave approval for field forces. • Managers can view feedback from the field force. • Field users update attendance, which determines route/ticket assignment. • Health and safety audit checks before and after activity.

Sr. No	Category	Requirement
		• Multiple image formats supported (CPE serial number, Customer Photos, etc.) • Tools for post-installation activities (Speed Test, Ping Gateway, Trace Path). • Mobile app supports offline data load. • Mobile app supports ticket creation. • Manager's mobile app has task management capabilities. • Patroller and FRT receive notifications for assigned tasks. • Patroller can view assigned route on the base map. • Check-in and check-out with selfies for Patrollers. • Patrollers can raise telecom faults, attach images, and managers assign tickets. • Mobile app supports live communication (Chat Box, SOS).
17	Measurement Book (MB)	• Mobile app for PIA's field personnel to record work details; cannot delete readings. • GFGNL personnel validate entries on-site via GFGNL MB app. • Integration with DGPS for accurate location tracking, compare measurements with GIS data. • IE performs Acceptance Test on measurements, discrepancies visible to PIA in web and mobile apps. • Includes Lengths, Profiles, Cable, Joint Pit/Manholes, Termination, and Splice Loss. • Geotagged images for documentation (e.g., splice loss, cable length). • Web app allows resolution of disputes between PIA and IE. • Assign unique codes to each PIA for tracking network work. • Visualize project timelines, task dependencies, milestones. • Track time spent and task relationships. • Define and track milestones with visual indicators. • Built-in chat for real-time communication, file sharing, and notifications. • Create custom reports based on project needs, KPIs. • Visualize project data on maps with charts (pie, bar, line, etc.). • Generate reports on progress by PIA across daily/weekly/monthly spans. • Graphical and geospatial comparison between planned and actual build data.

Sr. No	Category	Requirement
		• GFGNL Person validate network design and inspect work. • GFGNL Person can update plans with redlines, which are visible to GFGNL and PIA. • Preloaded templates for inspections, with pull-down comments and ability to attach free-text. • GFGNL Person can raise queries to PIA, and PIA can respond through their mobile app.
18	Project & Workspace Management	• Workspace Management • Project Managers and Team Owners can create Workspaces and define access permissions. • Workspaces should support team assignment, workflows, and notification templates. • Includes document containers, task templates, and task categories. Task Management & Visualization • Kanban Board and List View options for task management. • Tasks can be added from templates, copied, and duplicated. • Users can perform complete project planning, track progress, and assign tasks. Work log & Time Tracking • Automated and manual work log recording available. • Timer feature ensures only one active task tracking at a time. Communication & Collaboration • Private notes and public comments within tasks. • Chat functionality for stakeholder communication. Advanced Task Capabilities • Support for subtasks, sequential tasks, and recurring tasks. • Task scheduling, reminders, and delegation features. • Dynamic checklists that prompt users before completing tasks. Additional Functionalities • Geo-tagging for field service tasks. • Dynamic document containers for each task.
19	Training for Installation and Maintenance Staff	• Supplier provides training for the installation, operation, and maintenance of software tools. • All training materials provided in soft and hard copies. • At least 1 week of training for 25 personnel per batch.

1 Hardware Requirements

The bidder shall estimate the compute sizing required to meet requirements given in this tender and submit valid requirement to GFGNL. The Bidder shall be responsible to manage all the provided infrastructure to meet the requirements to operate and maintain for the contract period.

User Licence requirement:

For mobile GIS user, please consider the following User count for sizing purpose:

- During Implementation phase
- Concurrency: ~200 users
- Total user Count: ~1125
- During O&M phase Concurrency: ~100 users
- Total users Count: ~600

During Project Phase	**Zone**	**Project**	**Total Users asked**
New Ask	6	For PH III	1125+
During O&M Phase	**Zone**	**Project**	**Total Users asked**
New Ask	6	For PH III	600+

4.2 Operational Visibility Platform (NMS + OSS + BSS+ Network visibility):

Sr. No	Category	Requirement
1	System Overview	• The OVP will integrate with Element Management Systems (EMS) for optical IP node management. The proposed solution should work as a software layer/platform for the management of entire Bharat Net project in the state of Gujarat for the GFGNL. The proposed OSP solution should have complete functionality of Network Management System (NMS), Operations Support System (OSS), Business Support System (BSS) etc. or we can say it will be the combination of all these IT tools/system to fulfill the requirement mentioned in this section. The system shall serve a large-scale network. It must operate across multiple vendors while integrating with SNMP, SSH, and IP-based reachability for client and device management. • The Network Management System (NMS) shall be required to provide a scalable, automated, and vendor-neutral solution for network deployment, monitoring, and service management across multi-vendor IP and optical infrastructures. The system will streamline operations, ensure SLA compliance, and support end-to-end lifecycle automation with mobile-based deployment, GIS-based topology visualization, and OEM-engineer backed customization. • The proposed monitoring solution must feature a unified architectural

Sr. No	Category	Requirement
		design that seamlessly integrates functions such as: • Seamless new network deployments • Auto generation of configuration for new nodes and auto Integration. • Delta configuration updates for adjoining nodes. • SOP-based deployment for engineers with minimal skill requirements. • Comprehensive site deployment workflow with mobile-based features. • Centralized tracking and dashboards • Automated Network Environment Discovery- Auto discovery • Event and Alarm Management • Correlation and Root Cause Analysis • Reporting and Analytics • Operators must have access to an admin console with drag-and-drop automation for extracting fields from collected logs, minimizing complexities associated with parsing logs from various sources. • The platform must support customizable service-level reporting. Integration capabilities with email, SMS gateways, WhatsApp and third-party tools are required. • The solution should offer role-based, flexible dashboards that provide comprehensive information on a single page, including a map view. • Protocol Support SNMP v1/v2/v3 with AES 256 or higher, Syslog, XML, NETCONFIG • GFGNL will serve multiple department at a time, hence the Proposed solution should support multiservice monitoring model like simultaneously providing connectivity services to various scheme and systems of Government in Education/social justice/health/ Finance/ Transport /etc. department. • The proposed solution should be able to monitor the individual ISP Links for all hosted applications. Solution should have the ability to automatically detect Internet outages in ISP networks to help identify the problem area of outages. • The proposed visibility solution should support asked nodes in table 2 simultaneously monitoring capabilities for 24x7x365days for the contract duration.
2	Functional Requirements	Scalability & Multi-Vendor Support • The system must support at least 10 different network OEMs. • Custom onboarding must be available for integrating new OEM network nodes on demand.

Sr. No	Category	Requirement
		• The system should support the deployment of at least 20 professional engineers from OEM services for a minimum one-year period for customization and integration needs. Network Discovery, Network optimization & Inventory Management. • Auto-discovery of network nodes using SNMP, SSH, CDP, LLDP, Seed IPs, and Subnet Mask using NETCONF/YANG or equivalent for physical topology and service discovery. • Graphical inventory of physical and logical network components. • OEM - EMS-based management for optical IP nodes, falling back to SSH where EMS APIs are unavailable. • Automated traffic diversion to bypass degraded links. • Real-time bandwidth optimization across network segments. • Failure impact analysis for planned maintenance and service continuity. • Detecting and mitigating network congestion with traffic engineering. • Path computation and optimization Network Topology & Visualization • Network protocol-based topology diagrams. • GIS-based topology diagrams with GIS integration. • CDP, LLDP and BGP Topology • ISIS/IGP Topology • Lat-Long based Topology View • Network path visualization: a time-correlated, unified view of all paths between any two points on network. With visibility across network, application, routing, and device layers. • Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target. • The proposed solution should be able to clearly visualize the Hop-by-Hop visibility of the Underlay Network at a granular level Sub-Second) for Identifying clear problematic sections on the Glass pane view Deployment & Configuration Automation • Automated Deployment (AC): New nodes should be auto configured with minimal engineer intervention.

Sr. No	Category	Requirement
		• Delta Configuration Updates: Adjoining nodes should automatically receive delta configuration changes when new nodes are deployed. • SOP-Based Deployment: Engineers should only need to power up the device and connect cables. • Bulk Configuration Push: Network-wide configuration rollouts for standardization. Network Scanning • The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU. • Automated fault, performance and security management reports • Hierarchical network drill-down from NE to module- level configurations. • System backup and restoration mechanism for at least one month. Order & Inventory Management: • Streamlined order handling, automated provisioning, and real-time inventory tracking. • Network & Service Operations: Fault management, root cause analysis, impact assessment, and advanced fault correlation. • Customer & SLA Management: Efficient trouble ticketing, incident resolution, SLA compliance, and proactive issue handling. • Automation & Optimization: Workforce management, change control, and network discovery with reconciliation for operational efficiency. • Alarm Correlation & Root Cause Analysis (RCA), Incident Notification & Handling and Alarm Logging & Compliance • Security & Service Management including service provisioning, Inventory management, self-service portal and customer management • Work flow based process automation, API support for integrations, Log management etc. BSS Functionality • Proposed Business support system (BSS) should have detailed functionalities like Customer management, order-billing-revenue management, sales & marketing etc. It should work in tightly integrated manner with OSS, NMS and other modules.

Sr. No	Category	Requirement
		• Proposed solution should follow the standard Large IP network industry template from customer order generation to service provisioning. Activation to Billing and accounting to SLA management etc. It should cover each and every steps/stage in between the entire cycle irrespective of whether it is explicitly mentioned or not. These systems should be the one and only systems to manage the entire business of the GFGNL which ultimately fulfill the desires of self-sustainability and embarking on growth path to become most successful Large IP network in the state of Gujarat.
3	Helpdesk & Customer Issue Management & Problem Management	• The proposed tool must provide a structured, Latest ITIL compliant problem management framework, ensuring effective issue tracking, resolution, escalation, and reporting. It should support integration with incident, change, and configuration management while offering automated notifications, advanced analytics, and stakeholder communication capabilities. Compliance & Problem Record Management • Must adhere to Latest ITIL problem management best practices. • Capable of recording problem details, including date, time, source, contact, symptoms, and status. • Must support classification of problem records based on priority and category. Escalation & Workflow Management • Should allow automatic and manual escalation based on predefined rules. • Must enable linking of problem records to configuration items, support partners, or third-party vendors. • Problem records should be able to transition into a known error state when applicable. Integration with IT Service Management (ITSM) Processes • Ability to create problem records from incident records and link multiple incidents to a single problem. • Support for linking problem records to change records for better service lifecycle management. • Provide tracking and monitoring against defined tolerance limits, with notifications for breaches. Root Cause Analysis & Reporting • Must support one-click generation of Root Cause Analysis (RCA) reports upon problem resolution.

Sr. No	Category	Requirement
		• Separate review mechanism for major problem records to facilitate deeper investigation. • Advanced analytics tools for Pain Value Analysis, Risk Assessment, and Risk Mitigation Planning of TTs Built-in Root Cause Analysis Techniques • Should support methodologies such as: • Failure Mode and Effects Analysis • Fault Tree Analysis Stakeholder Communication & Notifications • Provide an option to announce workarounds and solutions to stakeholders efficiently. • Include an online operator reporting system and a helpdesk ticketing module for customer and network problem management. • Offer automated SMS, whatsapp and email notifications for any threshold breaches or urgent alerts • Communication to field members, customers and stack holders with voice call on single click
4	Network Topology & Visualization	• Network protocol-based topology diagrams. • GIS-based topology diagrams with GIS integration. • CDP, LLDP and BGP Topology • ISIS/IGP Topology • Lat-Long based Topology View • Network path visualization: a time-correlated, unified view of all paths between any two points on network. With visibility across network, application, routing, and device layers. • Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target. • The proposed solution should be able to clearly visualize the Hop-by-Hop visibility of the Underlay Network at a granular level Sub-Second) for Identifying clear problematic sections on the Glass pane view
5	Deployment & Configuration Automation	• Automated Deployment (AC): New nodes should be auto configured with minimal engineer intervention. • Delta Configuration Updates: Adjoining nodes should automatically receive delta configuration changes when new nodes are deployed. • SOP-Based Deployment: Engineers should only need to power up the device and connect cables.

Sr. No	Category	Requirement
		• Bulk Configuration Push: Network-wide configuration rollouts for standardization.
6	Network Scanning	• The proposed solution should support synthetic network test at both ends of a monitored path (GP to NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput--an improved form of the bandwidth metric--along with Path Visualization and path MTU.
7	Mobile-Based Site Deployment & Readiness Workflow	The system must support a comprehensive mobile-based deployment process, including: • Engineer Assignment based on site location. • Map-Based Navigation for engineers to reach deployment sites. • Mobile App-Based Site Readiness Checks before deployment. • Mobile App-Based Site Inspection & Survey with automated validation. • Mobile App-Based Remote ATP (Acceptance Testing Procedure). • Pictorial Proof of Site Deployment and Signoff via the mobile app. • All site deployment workflows must be centrally tracked on a dashboard.
8	Auto service Provisioning and monitoring	• Automated service provisioning. • Service Template Creation: Engineers should be able to model and create services with a no-code UI. • Automated Service Deployment: MPLS VPN, L3/L2 VPN, EVPN, ELAN and E-TREE services, Access policies, and IP address management (IPAM). • Real-Time Service Monitoring: Continuous SLA monitoring with alerting. • Multi-Vendor network Discovery: Auto-detection of network inventory running on different OEM devices. • Service quality detection for L3 EVPN and L2 EVPN VPWS, API.
9	Compliance & Policy Enforcement	• OS Compliance Monitoring: Ensuring network-wide version uniformity. • Automated Security Hardening: Enforcing NTP, AAA, SNMP, SYSLOG, and firewall security policies. • Audit & Remediation: Continuous compliance checks with auto-remediation.
10	Performance Management	• Performance KPI Reporting: Latency, jitter, bandwidth utilization, and link health monitoring.

Sr. No	Category	Requirement
		• Threshold-Based Alerts with automated troubleshooting recommendations. • The NMS should provide customizable KPIs and deep analytics for comprehensive performance monitoring. • It should enable end-to-end service quality monitoring, with predictive analytics that alert operators to potential issues before they impact services. • Historical performance data should be readily available for capacity planning and network optimization efforts. • Dynamic link and tunnel delay information.
11	Fault Management	• Network Fault Management • Server Performance Monitoring • Network Traffic Analysis • Centralized Log Management • Unified Dashboard Reporting • Incident Management • It must facilitate end-to-end asset lifecycle management, including AMC/warranty alerts, asset deletion with workflow integration, and incident logs linked to activity updates. • The NMS should support comprehensive alarm escalation and resolution workflows, ensuring that alarms are prioritized based on predefined criteria. • A fault history and analytics module should be implemented to provide proactive insights, helping identify and prevent recurring issues in the network. • Real-Time Fault Reporting with root cause analysis.
12	OS & Firmware Management	• Bulk OS Upgrades across network nodes. • Pre & Post Upgrade Validation. • Patch Management: Automating security patches across infrastructure.
13	SLA Monitoring & AI-Driven Analytics	• SLA Performance Dashboards with live metrics. • AI-Driven Predictive Analysis for network failure prevention. • Log Storage: 3 months searchable and 9 months Archive.
14	Reporting and Forensics/ analysis	• The system must support detailed reporting with drag-and-drop tools for custom queries and various formats (CSV, Excel, PDF). Reports must cover SLA compliance, MIS, and penalty calculations, as required by GFGNL.

Sr. No	Category	Requirement
		• The NMS should offer fully customizable reporting capabilities, enabling users to define parameters, metrics, and timeframes according to specific needs. • Reports should be exportable in multiple formats (e.g., CSV, PDF, Excel) and support scheduling for automatic generation and delivery. • Ad-hoc reporting should be supported to allow for flexible, on-demand analysis of network and service performance.
15	Log Management	• The proposed solution must classify logs consistently and provide an 8:1 compression ratio. It must support diverse log formats and offer SDK/REST API for custom connectors. Full-text search and forensic investigation capabilities are mandatory.
16	Software License	• Any Software upgrade change request shall be free of cost. GFGNL will not pay extra amount for upgrade or change request to deliver any functionality asked by GFGNL during contract period.
17	Configuration Management	• The NMS must support robust configuration management capabilities, including device configuration backups and rollback functionalities. • It should allow centralized configuration management, with full auditing capabilities to monitor and track configuration changes in real time. • Configuration templates must support both device-specific and service-specific configurations, ensuring efficient and error-free deployment across the network. • The platform must include a CMDB with asset lifecycle management, software license metering, and patch evaluation. Historical data retention must align with regulatory guidelines
18	Asset Management	• The NMS must provide end-to-end asset lifecycle management, from procurement to decommissioning, with integration to financial systems for accurate tracking of asset depreciation and warranties. • It should track both hardware and software assets, including licenses, providing visibility into the current status of all network resources.
19	Unified Console	• Infrastructure metrics and logs must be tightly integrated into a single consolidated console for managing infrastructure and security events. • The NMS should provide open and flexible integration interfaces (e.g., REST APIs, SNMP, XML) for easy integration with third-party systems. • The system must be capable of integrating with both legacy and future technologies, enabling seamless data exchange and interoperability. • Real-time data exchange protocols should be supported to ensure smooth and efficient integration with other management platforms.

Sr. No	Category	Requirement
20	Security & Accounting Management	• The NMS should include encryption for sensitive data, support multi-factor authentication, and adhere to security best practices for user authentication. • Detailed access logs, audit trails, and compliance reports should be available for security auditing and regulatory compliance. • Integration with external identity management systems is required to manage user roles and permissions centrally. Data Security • Log data must be stored centrally without reliance on third-party databases, ensuring control over collected data and SLA calculations. Data retention must comply with DOT/GOG/GOI guidelines.
21	Non-Functional Requirements	• High Availability: 99.99% uptime with redundancy. • API & EMS Integration: RESTful API support for third-party integrations. • AI-ML Use cases: Functionality desired for futuristic use cases but not mandatory. • Security: Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Encrypted Communication.
22	Network visibility	• Refer backhaul RFP Section service performance monitoring (Qualitative service Visibility) all the specified functional requirements to be adhered
23	Standards	• OSS tool should be certified TEC-GR-IT-NMS-003-01-NOV-15, comprehensive eTOM coverage

- **MIS:** solution should be able to generate the following reports but not limited to: -

Sr. No.	Report Type / Category	Specifications	Periodicity
1	Dashboard Reports	Shows N/W availability, Average BW available vs Usage per GP, Latency, Jitter. Custom dashboards for Senior Management & Field Offices in a readable format.	Daily
2	Bandwidth Availability & Utilization	Available bandwidth per of Router, ONT, OLT, Mini OLT and switch devices Taluka/Block-wise, District-wise, and State-wise. Bandwidth Utilization (Max, Min, Avg) per GP Ring, Block Ring, and District Ring.	Daily
3	Device Availability & Performance	Availability of Router, ONT, OLT,Mini OLT and switch devices (Live vs Faulty) PoP-wise, Block-wise, District-	Daily

Sr. No.	Report Type / Category	Specifications	Periodicity
		wise, and State-wise. CPU, Memory, and BW utilization of Routers & Switches.	
4	Fault & Incident Management	Total No. of Complaints Raised. Trouble Ticketing & Life Cycle Management for Network & Service Problems. Ageing Report of Issues/Complaints/Incidents.	Daily & Monthly
5	Network Performance & Monitoring	Network KPIs (Up/Down Status), SLA Monitoring, Real-time Traffic Monitoring, Threshold Alerts, and Zoom-in Analysis down to the port and IP level. Historical reports for various periods.	Daily & Weekly
6	Receive Signal Strength Monitoring	ONT/Router/Mini OLT signal strength tracking with alert triggers when below the defined threshold.	Daily
7	Configuration Management	Auto discovery of devices, Resource Inventory Management, Service Template Management, and Configuration Change Reports.	Quarterly
8	Preventive & Scheduled Maintenance	Preventive maintenance reports, Scheduled maintenance tracking, and Software upgrade/enhancement reports.	Quarterly & Monthly
9	Security & Access Management	Role-Based Access Control (RBAC), Operator Authentication, Audit Logs, Helpdesk Module with SMS/Email Notification.	As Required
10	Network Topology & Mapping	End-to-end network topology connectivity till the last mile CPE, dynamic discovery of fibre connectivity.	As Required
11	Inventory & Asset Management	Inventory Reports including Dark Fiber Availability, Number of Fiber Used, and Penalty Calculation. End-to-end Asset Lifecycle Tracking including hardware, software, and license management.	Quarterly
12	Reporting & Data Extraction	Reports with drill-down features (package-wise, district-wise, block-wise, ONT/Router/Mini OLT and switch -wise). Tabular and Graphical reports with extraction in Excel, CSV and PDF format.	D/W/M/ Q/Y
13	SLA Compliance & Billing	SLA monitoring, SLA computation, and SLA-based billing generation for partners and end clients. Penalty % of O&M amount tracking.	Quarterly

Sr. No.	Report Type / Category	Specifications	Periodicity
14	Service Performance & Uptime Analysis	Service Availability, Downtime, Usage/Utilization, Fault & Rectification, Performance Statistics, and % Uptime Achieved.	As Required
15	Compatibility & Integration	NMS should support SNMP, JAVA, CORBA, XML, REST API, and integration with OEM APIs. The system must support both legacy and future technologies for seamless data exchange.	As Required
16	Any Other Reports	Within the reporting framework with flexibility of rapid customization.	As Required

4.3 Network Intrusion Prevention System (NIPS)

Sr. No	Category	Requirement
	Architecture	• The NIPS should have integrated redundant hot swappable fan tray and dual redundant power supply to remove any single point of failure in the solution also proposed NIPS component should not use common firmware/underlying OS used for NGFW to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.
2	Interface & Performance	• The proposed appliance should have minimum of 8 x 1/10/25 Gigabit SFP+ ports with Short Range transceivers and additional network module supporting atleast 4-port 40/100 Gbps QSFP28/QSFP. Also support hardware fail open cards for critical interfaces and appliances level. • The proposed single appliance should deliver 100 Gbps of real- world Intrusion Prevention System (IPS) Inspection throughput scalable upto 400 Gbps on stacking supporting 300M Concurrent Connections/Sessions and supporting atleast 40 Gbps TLS/SSL scalable up to 200 Gbps throughput on stacking having <60 microsec latency
3	Functionality	• Should support to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption and memory errors also should support inspection of Asymmetric traffic consisting jumbo frames, DGA Defense filters, Machine learning, Virtual patching capability • 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,

Sr. No	Category	Requirement
		malicious IP addresses, hosts etc. for correlation and blocking in the NIPS. • Should support automatic Real Time Signature update within few seconds without human intervention considering global threat intelligence having capability to trace action set to extract a private key from the network flow in order to help restore encrypted files to the victim while blocking traffic to the CnC server • Should support custom application signature supporting running applications in datacenter environment detection mechanism to optimize security effectiveness • Should support 20,000 (excluding custom signatures/filters) IPS signatures/filters or more. The signatures/filters should also have categorization i.e. exploit, vulnerabilities, rconnaisance, identity theft etc. • Solution must support IP reputation intelligence feeds and custom lists of IP addresses including a global blacklist.The solution should have the capability to detect hash-based detection mechanism to detect any malicious traffic pattern • Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly • The solution vendor must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection • Should support VA scanners (Qualys, Rapid 7, Nessus) integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality. • Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure
4	Temperature & Humidity	• Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing

4.4 DDoS - Distributed Denial-of-Service

Sr. No.	Requirement
1	The proposed solution should be a dedicated solution as DDoS protection device, not as add on license Feature on ADC and NGFW.

Sr. No.	Requirement
2	should support 16x10GbE SFP+ ports, 4x10G SX-SFP+ bypass ports, Dual Power supply & 4TB SSD.
3	Device should support at least 80Gbps throughput
4	The proposed solution should have the capability to be configured in detect as well as protect mode.
5	The proposed solution should prevent suspicious traffic for threats and blocking malicious traffic.
6	Should protect ICMP attacks: ICMP floods, ping floods, smurf, IP Spoofing, LAND attack, Teardrop, IP Option Timestamp, IP Option Route Record, IP Option Source Route, Ping of Death, Tracert, ICMP Redirect, ICMP Unreachable, ICMP Large Packet.
7	The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack
8	Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, Defense Win Nuke, TCP Error Flag
9	Should protect UDP based attacks: UDP Flood, UDP Fragement Flood, UDP Fingerprint, Fraggle, UDP Large Packet
10	Should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation
11	Should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense, DNS NxDomain Defense, DNS Query Flood Defense , DNS Reply Flood Defense, DNS TTL Check , DNS Source Authentication.
12	The solution should support Brute Force attack mitigation
13	The solution should support the behaviour based DDOS mitigation.
14	The solution should provide the traffic AUTO learning function for the DDOS traffic monitoring
15	The traffic Auto learning threshold can be apply automatically after auto learning completed.
16	The solution should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type.
17	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,
18	The solution should support Access control list based on inbuilt GeoIP with configurable duration.
19	The solution should able to import third party IP database through File or URL.

Sr. No.	Requirement
20	The system should support IPv4 and IPv6 dual-stack without deteriorating performance
21	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP
22	The solution shall be able to immediately support both IPv4 and IPv6, and implements dual stack architecture.
23	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.
24	The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2
25	The solution must provide the latest Management Information Base (MIB) file for SNMP operation.
26	The solution log shall contain the following information: Attack logging like Source IP, Destination IP, Destination Port, Group Name, Service Name, Protocol Attack Type, Action , Anomaly Count, DDoS Attack and logging to Syslog
27	The solution shall provide the flexibility of performing configuration via GUI and command base remotely.
28	The solution shall be able to export syslog to existing syslog server and SIEM system.
29	The solution shall be able to support user authentication based on Local Password, RADIUS & TACACS+
30	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region
31	The solution must be able to generate summary attack report of daily/weekly/monthly
32	The solution must provide packet capture for debugging.
33	The solution must support the generation of pdf reports containing the detailed statistics and graphs

Note: Any equivalent open protocols or technical terminologies are allowed.

4.5 Link Load Balancer

Sr.No.	Category	Specifications
1	**Features**	Should be high performance purpose built dedicated next generation hardware to load balance traffic from different ISPs. Support for multiple internet links in Active-Active load balancing and active-standby failover mode.
		Appliance should support 16x10GbE SFP+ ports, 2x40GbE QSFP+ ports & The appliance should have 64GB RAM and 4 TB SSD.

		Platform should support Minimum 55K SSL TPS for RSA 2048 bit key and 38K SSL TPS for ECC (ECDSA-SHA256).The appliance should have minimum 100Gbps of system throughput from day one. Or Bidder may increase the throughput, ports, storage capacity to meet the operational requirements
		Appliance must have link load balancer license & server load balancer license comes by default along with base license including ipv6. Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, hash ip, target proximity and dynamic detect
		Standard policy to implement business logic on network without changes in application code. Should support Outbound & inbound load balancing algorithms like round robin, Weighted round robin, proximity.
		Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links. IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation, Domain name support for outbound link selection for FQDN based load balancing.
		Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks. Health check for intelligent traffic routing, failover. In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links. Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.
		Should support various deployment modes for seamless integration including reverse proxy (IPv6 to IPv4, IPv4 to IPv6) and IPv6 to IPv6 transparent and reverse proxy mode. Should support persistency features including RTS (return to sender) and ip flow persistence.
		Security should support advance ACL's to protect against network based flooding attacks, define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value utilizable for the clients on a specified subnet/IP or network.
2	**Security**	should support advance ACL's to protect against network based flooding attacks, define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value utilizable for the clients on a specified subnet/IP or network.
		Should support QOS for traffic prioritization and provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. support rate shaping, integrated firewall module to protect the device itself from network based DOS and DDOS attacks. Also, security features like reverse proxy firewall, Syn-flood and dos attack protection

		features from the day of installation .
		Solution should support DDoS attacks like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapse (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic
3	Global Load balancing	The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one
		Capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc. GSLB solution should able to evaluate round trip time (RTT), Packet loss ration (PLR) and hop count for dynamic proximity calculations.
		The appliance should support global server load balancing algorithms including - Weighted round robin, Weighted Least Connections, Administrative Priority, Geography, Proximity, Global Connection Overflow (GCO),Global Least Connection (GLC),IP Overflow (IPO), should support dynamic proximity and static proximity rules to direct the traffic to closest datacentre/DR/Defined locations.
		Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.
		GSLB SDNS should provide full IPv6 functionality with support for AAAA DNS resolution, proximity rule support for IPv6 , dynamic proximity (to detect IPv6 local DNS's) and SDNS health check for IPv6 service IP's
4	**High Availability**	Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.
		Stateful session failover with N+1 clustering support when deployed in HA mode
		Support for multiple communication links for realtime configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc.. and heartbeat information
		should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speed up the failover. should

		support for secondary communication link for backup purpose
		should support floating IP address and group for stateful failover support. Appliance must have support 256 floating ip address for a floating group
		should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot. should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway. Configuration synchronization at boot time and during run time to keep consistence configuration on both units.
5	**Management**	The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality, should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting. provide detailed logs and graphs for real time and time based statistics. multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. support led warning and system log alert for failure of any of the power and CPU issues. Should support XML-RPC for integration with 3rd party management and monitoring of the devices.

Note: Any equivalent open protocols or technical terminologies are allowed.

4.6 Next Generation Firewall:

Sr. No	Category	Requirement
1	Architecture	• The proposed NGFW solution be a dedicated rack mounting appliance. • The offered firewall must be a dedicated/single appliance and should be provided with redundant hot swappable power supplies within the NGFW appliance.
2	Interface & Requirement	• The firewall should have minimum 4 x100/40G,12x10G/25G and 6 x1G/10G supported interface from day 1 with fully populated SR transceivers as per the ports. • The Firewall appliance should include the ability to support High availability: Active/Active, Active/Passive and HA clustering support.
3	Performance Capacity	• The Appliance must handle the threat prevention throughput of minimum 60 Gbps enabling security features and measured with Enterprise Mix / Application Mix traffic. • The Firewall must deliver minimum 80 Gbps of IPSEC throughput from day 1. • The Appliance should support minimum New Connections per Sec of 1 million.

Sr. No	Category	Requirement
		• The Application should have Concurrent Sessions of – 60 million from day one.
4	Next Generation Firewall Features	• NGFW solution should have the security features including IPS, Application control, Anti-Bot, DDOS prevention, Anti-Malware, Web filtering, DNS security, Sandboxing • The IPS/Anti-Bot must be able to detect botnets based on signatures and anomaly based detection. • The proposed firewall shall be able to implement Zones, IP address, Port numbers, User ID/Application ID. • The proposed firewall shall be able to protect the user from the malicious content upload or download by any application.
5	Threat Protection	• All the proposed threat functions support like Full-Steam Deep Inspection, Anti-Evasion Defence, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Vulnerability Exploit Detection, Custom fingerprinting/Signature, Anti-Botnet and DoS/DDoS Protection. • The proposed firewall shall support stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections. • The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window can be schedule or automatic • Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, pop3, ftp traffic with configurable AV action such as allow, deny/drop, alert etc. • NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time. • IPS must deliver more than 10000 IPS rules/Signatures for detecting exploit attempts against known vulnerabilities. • Firewall Services with Access Lists and time-based Access lists/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

Sr. No	Category	Requirement
		• Should provide complete protection by performing full decryption and inspection of TLS/SSL. Should support TLSv1.3 decryption • Should provide complete protection by performing full decryption and inspection of TLS/SSL. Should support TLSv1.3 decryption • The Device should be capable of SSL exclusion of selected applications.
6	Network Address Translation & IPv6 Support	• The proposed firewall must be able to operate in routing/NAT mode. It must be able to support Network Address Translation (NAT) and Port Address Translation (PAT). • The NGFW should Support IPv4 and IPv6 from day one. • The NGFW solution should support NAT64, NAT46, NAT66, DNSv6 & DHCPv6
7	Routing and Multicast support	• The NGFW should Support L3 protocol functionality like Static Routes, OSPFv2/OSPFV3, BGP V3/V4, Policy Based routing, Tunnelling and NAT from day one. • The device should support Multicast routing
8	Authentication	• Support various form of user Authentication methods simultaneously, including Local Database, LDAP, RADIUS, Windows AD & Single Sign On and SAML. • ISP WAN Link-Load balancing and Fail-over with Multiple Links, Application based load balancing, Fail-over based on parameters such as Latency, Jitter, Packet-Loss, QoS / Bandwidth management.
9	Monitoring, Management and Reporting	• The solution should come with a web-based administration interface or GUI console and CLI. Solution must be able to define the Custom roles. • Bidder to propose separate on-premises dedicated logging & reporting solution from same OEM (Virtual /Physical Appliance) • In Case of Virtual Appliance, bidder to consider required computing / hardware resource for the VM with having storage capacity to store the logs of minimum last 6 Months. • Should have options to generate Predefined or customized Advance reports in different formats. • Solution should have configurable options to schedule the report generation. • Should provide granular logs and filtering options.
10	Equipment Test Certification	• IPv6 Certification, ICSA/ EAL3+/NDPP or Common Criteria Offered firewall should have valid MTCTE certificate
11	Support, Warranty	• The Appliance shall be offered with the comprehensive warranty and technical support for minimum five years from the date of FAT/Go-Live.

Sr. No	Category	Requirement
		• The NGFW should be proposed with 7 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, URL Filtering, DNS Security, include all other require licences to achieve features as mentioned above from day 1 from the date of FAT/Go-live. • Power Required ---- AC- 200 V-240 V AC, 50/60 HZ • Temperature Range/Humidity------ 0°C to 40°C / Humidity levels of 10% to 90% non-condensing • 7+3 extendable years 24x7 comprehensive warranty from the OEM from day one. • TEC 49090:2023 or latest Tech GR
	Note:- Any equivalent open protocols or technical terminologies are allowed.	

4.7 BNG:

Sr. No	Category	Requirement
1	General capabilities	• A redundant hardware should be provided with Redundant control plane & forwarding should be included in the router. • The user plane / data plane solution should have minimum 8 Tbps switching capacity with 2200 Mpps forwarding performance. • The solution should have minimum 80 k subscriber per user plane, scalable option with multi chassis for expansion should be supported. • The solution should have capability to configure and manage the subscriber from the central NoC. • The solution should be able to support IPoE and PPPoE subscribers. • The solution should be capable of minimum 200 connections per seconds. • The solution should be capable of local breakout of the traffic for internet. • The solution should have external NAT capability. • Bidder can quote a CUPS solution or equivalent. • The solution should be capable to provide Dual Stack subscribers at day one. • Solution should be capable of destination based billing & metering support, differential treatment for YOUTUBE, OTT, etc. • Solution should support deterministic & Non-deterministic logging as per DOT guidelines. • Bidder should provide BNG network element management system and should provide open northbound interfaces for OSS/BSS integration.

Sr. No	Category	Requirement
		• TEC/GR/IT/TCP-005/01/MAR-14 or latest Tech GR
2	Architecture	• CP and UP communication SHOULD be on PFCP and GTP-u interfaces as defined by BBF in TR459 • The DBNG solution MUST support Control and User Plane Separation Architecture (CUPS) or equivalent. • DBNG Control Plane must be cloud native based with multiple PODs allowing scale in and scale out of individual functions independent of each other. • Supplier must specify maximum number of nodes possible in K8s cluster for specific cNF deployments.
3	Subscriber Plane	• SUBSCRIBER PLANE SHALL be able to support IPoE DHCP model • SUBSCRIBER PLANE SHALL be able to support PPPoE model • HTTP Redirect support • Supplier MUST provide a list of all the state information CP maintains internally for each connected user • SUBSCRIBER PLANE SHALL be compliant with Dynamic Host Configuration Protocol (DHCP) specification (RFC 2131) • SUBSCRIBER PLANE SHALL support IPv6 in all scenarios including Dual-Stack IPv4/IPv6 • BNG SHALL be able to force IP address renewal, based on configurable rules • BNG SHALL be able to force IP address change at a configurable time range • SUBSCRIBER PLANE SHALL support a configurable DHCP lease time • DHCP lease database MUST be stored in non-volatile storage and preserved across system reboots/restarts • SUBSCRIBER PLANE SHALL support limiting the number of IP addresses that can be assigned to a subscriber. • Supplier MUST provide a list of Supplier Specific Attributes (VSAs) used by the RADIUS interfaces • SUBSCRIBER PLANE SHALL support the configuration of non-standard ports for RADIUS authentication and accounting • It MUST be possible to add the Accounting-Session-Id attribute in the RADIUS Authentication Access Request • SUBSCRIBER PLANE SHALL support the RADIUS Class attribute • SUBSCRIBER PLANE SHALL add the IP address allocated to the subscriber into the Start Accounting message

Sr. No	Category	Requirement

		• SUBSCRIBER PLANE SHALL implement the Accounting On/Off mechanism.
		• SUBSCRIBER PLANE SHALL be able to add, in the RADIUS Calling-Station-ID or NAS-Port-Id attributes, the L2 circuit ID (e.g. slot/port/VPI/VCI) and/or the DHCP option 82 value
		• SUBSCRIBER PLANE SHALL support the RADIUS Change-of-Authorization (CoA) message, in order to update the subscriber session service profile, without disconnecting the session
		• SUBSCRIBER PLANE SHALL support the RADIUS Disconnect-Request message in order to disconnect the subscriber session or service
		• The subscriber session re-authorization MUST support at least the update of the following subscriber services / attributes:
		  ◦ IP Access List
		  ◦ Session and Idle timers
		  ◦ Upstream/Downstream Rate Limit
		  ◦ IP Queuing policy
		  ◦ Policy Based Forwarding
		  ◦ HTTP Redirect
		• Shall be supporting the RADIUS RFCs like RFC 2284 , RFC2809, RFC2867, RFC2868, RFC2882, RFC3162, RFC3576, RFC3579, RFC5176, RFC3162,RFC5515
		• Support to configure more than one RADIUS servers (Accounting and Authentication), one acting as primary and the other/others as backup servers and support the configuration for using –if needed- different servers for Accounting/Authentication/Authorization.
		• Subscriber plane shall be able to re-authorize the subscriber sessions without disconnecting the session itself

4	Reliability	• Supplier MUST specify the redundant components available in the Subscriber plane. • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover)
5	Lawful Interception	• Supplier shall specify the redundant components available in the Subscriber plane. • Any failover procedure in Subscriber plane shall preserve the subscribers' sessions (Hitless Failover) • SUBSCRIBER plane shall provide dedicated interfaces for lawful interception of traffic coming from any interface or going out to any interface on any of UP connected to it. The redirection should take place directly from UP and should not be via SUBSCRIBER plane.

Sr. No	Category	Requirement
		• SUBSCRIBER plane shall also be able to select traffic for lawful interception, based on the subscriber access node/port. • Supplier shall specify which parameters are available regarding traffic selection for lawful interception.
6	Management	• Subscriber plane shall support Network Time Protocol (NTP), as defined in RFC 1305, and Supplier shall specify NTP synchronization precision • The metrics should include subscriber status, count, pod/vm performance etc. • Any equivalent open protocols or technical terminologies are allowed.

4.8 Carrier Grade NAT:

Sr. No	Category	Requirement
1	Hardware Architecture	• The appliance-based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one • The appliance should have at least 16 * 10G Gigabit ports from Day one • The appliance should support 2 x 100G interfaces for future usage • The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory
2	Performance & Scalability	• CGNAT should support 22 million translations for NAT44, NAT 64 etc. • CGNAT should support more 50 Gbps per chassis
3	Functionality	• 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
4	Security Features	• Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc • Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat • Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality • Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6

Sr. No	Category	Requirement
		• Should support Multicast protocols like IGMP, PIM, etc • Should support capability to integrate with other security solutions to receive contextual information like security group tags/names • Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. • Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware. • Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. • Should be capable of detecting and blocking IPv6 attacks. • Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control • Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., Net Flow) and the ability to detect deviations from normal baselines. • The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor • Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist • Should must support DNS threat intelligence feeds to protect against threats • Should must support URL threat intelligence feeds to protect against threats • Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories. • Should support safe search for YouTube EDU enforcement • Should support the capability of providing network-based detection of malware by checking the disposition of known/unknown files using SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance (if required in future)

Sr. No	Category	Requirement
		• The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection. • The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). • Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location • The detection engine should support the capability of detecting variants of known threats, as well as new threats • The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. • Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
5	Management Functions	• The management platform must be accessible via a web-based interface and ideally with no need for additional client software • The management platform must be a dedicated OEM appliance and VM running on server will not be accepted • The management appliance should have 2 x 10G port and integrated redundant power supply from day one • The management platform must be able to store record of 15000 user or more • The management platform must provide a highly customizable dashboard. • The management platform must domain multi-domain management • The management platform must provide centralized logging and reporting functionality • The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows • The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication. • Should support troubleshooting techniques like Packet tracer and capture • Should support REST API for monitoring and config programmability

Sr. No	Category	Requirement
		• The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. • The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG). • The management platform must support 8 GB logs/day for period of 4 months • The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. • The management platform support running on-demand and scheduled reports • The management platform must risk reports like advanced malware, attacks and network • The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

- Any equivalent open protocols or technical terminologies are allowed.

4.9 Core Router:

Sr. No	Category	Requirement
1	Architecture	• The router shall support a redundant and scalable architecture, including CPUs, modular power supplies, and performance components. • All interface modules and power supplies shall be hot-swappable and provided with 1+1 route processor, 1+1 or 1+N switch fabric and power supply redundancy.
2	Interface and Performance	• It shall also support minimum non-blocking capacity of minimum 2 Tbps full duplex per slot and 6 Tbps chasis throughput. handle minimum 256K IPv4 and 128K IPv6 routes per line card • It shall have minimum ports 8 *100 G and 14*10G (spread across two line cards equally) and should support 6 x 400G and when required with change of pluggable & addition of license and may be extended in future as per requirement. • The router shall provide wire-rate throughput on all interfaces, with sufficient optical distance to eliminate the need for additional equipment

Sr. No	Category	Requirement
		• The router should also support 100G DWDM / RON, 200G DWDM/ RON, 400G DWDM / RON interface capabilities from day 1, final number of required interfaces will be decided based on DWDM planning requirements finalized by DWDM RFP SI. • Specifications can be collected from Backhaul upgrade RFP on GFGNL website.
3	Functionality	• The router shall support traffic classification, congestion management, traffic conditioning, hierarchical QoS policies and various other security features to prevent network attacks and vulnerabilities The router shall support access control lists to filter traffic based on parameters, per-user authentication, authorization and accounting. • The router shall support multicast, routing and protocols • The router shall be TEC-GR: TEC 48050:2024
4	Routing and protocols	• Complete stack of IPv4, Static routing (IPv4 & IPv6), Dynamic routing IP v4 and IPv6 (BGP, OSPF, IS- IS) VRRP and BGP Prefix Independent Convergence (EDGE and Core). The router must support multiple instances of protocol OSPF (v2 & v3) and IS-IS. Also support link aggregation into single bundle. Boot options like booting from TFTP server, Network node & Flash Memory. Router support both L2 and L3 services on all interfaces • Shall have Multicast routing protocols IGMPv1, v2, v3, PIM-SM and PIM-SSM, MSDP, IGMP v2 snooping. The router should support SNMP/Netconf, YANG, gRPC and other modern system management protocol • Complete stack of MPLS provider/provider edge functionality i.e MPLS VPN, mVPN, AS VPN, Diffserv tunnel modes, MPLS, Inter AS VPN, VPLS, OAM, Ethernet OAM, Ethernet over MPLS. Segment routing and segment routing traffic engineering. PCEP, SyncE & IEEE1588v2. Also support Point-to-Point and Point-to-Multipoint LSP for Unicast and Multicast traffic. support minimum 3 ECMP paths - equal cost multipath. • Shall support MPLS Provider/Provider Edge functionality. MPLS VPN, MPLS mVPN (Multicast VPN), AS VPN, DiffServ Tunnel Modes, MPLS TE (Fast re-route), DiffServ- Aware TE, Inter-AS VPN, Resource Reservation Protocol (RSVP), VPLS, VPWS, Ethernet over MPLS, EVPN, Segment routing and Segment Routing Traffic engineering, CFM (IEEE802.1ag), Link OAM (IEEE802.3ah) and Y.1564, ITU Y.1731 The device should support YANG - A Data Modelling Language for the Network Configuration • Segment routing, SR TE, SR PCE, SR ODN, Anycast SID, Binding SID,TI-LFA, R-LFA, IP-FRR, BGP-LS and PCEP.

Sr. No	Category	Requirement
		• Note : Any equivalent open protocols or technical terminologies are allowed.
5	Network device manageability	• The solution should support the network configuration protocol (NETCONF) that provides mechanisms to install, manipulate, and delete the configuration of network devices • The router should support telemetry based on push model for monitoring network devices. The router should support sending telemetry data to multiple consumers simultaneously. The solution shall use either UDP or GRPC for transport of telemetry data. • The Router should support various software models/sensors for capturing different health • Parameters from the devices, based on either yang, xml or open config
6	QoS	• The router should support jumbo frame, port mirroring – local and remote, DHCP Server and DHCP Relay function. QoS features: classification and hierarchical scheduling, WRR, strict priority (SP), profiled scheduling and multi-tier policing and shaping. QOS shall be supported for all type of interface including Bundled interfaces. • Support multi-level of access privileges through Local database and through an external AAA Server. Shall support SSHv2. router shall support QOdS and HQOS for L2 & L3 service on all kind of interface.
7	Temperature & Humidity	• Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing

Note: Any equivalent open protocols or technical terminologies are allowed.

4.10 Core Switch:

Sr. No	Category	Requirement
1	Architecture	• The switch shall support non-blocking Layer 2 switching and Layer 3 routing, providing 1:1/N+1 redundancy for power supplies, fan trays and fan. • 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. • The switch should be a chassis based switch and should have at least 6 payload slots. • The Switch should have a minimum 2.4Tbps of non-blocking performance. • The Switch should support non-blocking architecture, all proposed and equipped ports must provide wire speed line rate performance

Sr. No	Category	Requirement
		with Zero Touch provisioning and capability to support fully customizable ZTP script, downloadable at start-up of the system based on the DHCP options.
2	Interface and Performance	• The switch shall support minimum 24 x40/100G on day 1 and also support additional line cards for future expansion. • The switch should support a variety of interfaces such as 1/10/25/40/100G either natively or via breakout. • All necessary breakout cables to be included along with the switch. console port, and management interface for Out-of-Band Management populated with necessary optics as per proposed solution. • It should support breakout on all ports • The switch should have line rate performance for the asked port combinations. • TEC GR 480060:2023
3	Functionality	• The switch shall support multicast, routing and protocols required to run services • It should support sufficient Ipv4 a-nd Ipv6 routes and hardware-based load balancing, as per requirement • The switch shall support classification and marking, methods for identifying traffic types, and real-time traffic differential treatment and support hierarchical QoS policies • The switch shall support port-based authentication from Layer 2 to Layer 4, control plane protection, stringent security policies, AAA and various other security features to prevent network attacks and vulnerabilities. • The switch shall support remote login using Telnet and SSH V.2 • Support layer 2 extension over VXLAN across all Data Centre to enable VM mobility & availability and support BGP EVPN Route type-1 to type-5 for the overlay control plane. • Switch should support at least 512 IP-vrf instances and 4K Mac-vrf instances, 250K Ipv4 LPM routes, 32 MB Packet Buffer. • Capability to access underlying Operating System (OS) tools and management (e.g. bash, cron). Shall support YANG and gRPC/Gnmi/ interface. • Should support BGP, MPLS, OSPF, Ipv4, Ipv6, static and dynamic routing, mBFD on LAG interfaces.
4	Temperature & Humidity	• Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing

4.11 Access Switch:

Sr. No	Category	Requirement
1	Architecture	• The switch shall support non-blocking Layer 2 switching and Layer 3 routing to ensure seamless data flow across the network.

Sr. No	Category	Requirement
		• It shall support 1:1/N+1 redundancy and reliability for critical features such as power supplies and fans to eliminate single points of failure.
2	Interface and Performance	• It shall support high-speed connectivity equipped with 20 x 10/ 25G Fibre and 4 x 40/ 100G ports, enabling high-speed data transmission and scalability. • It shall support line rate performance for the asked port combinations.
3	Functionality	• It shall support scalable routing and capable of handling sufficient IPv4 and IPv6 routes, as per requirement • It shall support load balancing ensuring optimal traffic distribution and performance • It shall provide robust security with port-based authentication, control plane protection, and support for external AAA databases. Includes comprehensive management features like SNMP v2/v3, centralized syslog, and packet capture capabilities. • The switch shall support multicast, routing and protocols required to run the services • TEC/48060:2023
4	Temperature & Humidity	• Operate within a temperature range of 0 to 40 degrees Celsius and humidity levels of 10% to 90% non-condensing

Note:- Any equivalent open protocols or technical terminologies are allowed.

4.12 AAA Server:

Sr. No	Category	Requirement
1	General	• AAA Solution should be a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a Single platform. AAA solution should compliant with Telecom Regulatory Standards/GOI and Cybersecurity standards of India. AAA should support Cluster deployment provides High Availability (HA) solution from day one.
2	Functionality	• The proposed solution should allow to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise • Should support multiple Admin Group Roles and responsibilities like Helpdesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin, Read-Only Admin and System Admin • The proposed solution should support a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via

Sr. No	Category	Requirement

		Secure Tunnelling (FAST), TEAP, and EAP-Transport Layer Security (TLS
		• The proposed solution should provide complete guest lifecycle management by empowering sponsors to on-board guests
		• The proposed solution should support different conditions for TACACS+ or Device Administration Policy –
		  • Device Network Condition(IP Address/ Device type/ Device Group)
		  • Device Port condition (IP Address, Device, Network Device Group/Port used)
		  • Simple/Compound Condition – End-user/End-user Group/Time of the day/office hours etc)
		• The proposed should support TACACS+ protocol for authorization of each command executed on the shell of the routers & switches.
		• The proposed solution should support on-demand health-check of the hardware nodes
		• The proposed solution should support the backup and recovery of policies/configuration
		• The proposed solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).

3	Logs and Reports	• AAA Should have the ability to create necessary logs of user sessions and generate various reports based on the same. Logs should have details like Login/Logout Date & time, MAC Address, Device type, Nos of persons to whom Wi-Fi services denied with reasons, Total internet bandwidth used by all free & paid Wi-Fi users, mobile numbers, users login, Survey based login, Email & SMS OTP
4	Protocols	• AAA should support authentication protocols, including PAP, MS-CHAP and standard security protocols.
5	Compatibility with gateways	• 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.
6	Interface and compatibility with OEMs	• AAA Should have GUI for configuration, Rule base engine for different Flow, able to Integrate over standard RADIUS protocol with multiple OEM products, MAC Provision and Authentication. Support MACID based Authentication via Captive Portal, support Web Self-care-based login using existing username password, Usage collection from multiple network setups/Groups/topology, Workflow based system with – Configurable Authentication & Authorization for different Networks
7	Audit	• AAA Should Support Audit of all Customer & Staff activity.
8	Subscriber profile	• AAA should support Seamless roaming with proxy forwarding based on Realm, ANI & DNIS or any other standard methods. Also, handle requests from Partner networks/devices and authenticates for roaming. AAA should provide Subscriber profile lookup based upon network across multiple type of repository like LDAP, RDBMS, file based etc

Sr. No	Category	Requirement
9	Alerts	• AAA should provide Alerts & notifications via SMS, email, Web Self-care with configurable/customize templates
10	Access and authentication security	• AAA should be Access Agnostic Architecture for handling requests from multiple ISP partner networks/multiple devices.
		• AAA should provide Workflow based Authentication & authorization flows for each type of ISP/Telco partner network. Pre & Post Auth Plugins to manage demands of uniform service management across multiple networks
		• AAA The solution must allow for the complete separation of Authentication and Authorization from different sources. For example, authentication against Active Directory but authorize against Local database etc.

Note : Any equivalent open protocols or technical terminologies are allowed.

4.13 Virtualization solution:

Sr. No	Requirement
1	Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS for greater reliability and security.
2	Virtualization software shall allow heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (Red Hat, SUSE, Ubuntu, CentOS - all of these)
3	Virtualization software should have the ability to live migrate Virtual machines files from one storage array to another without any Virtual Machine downtime. It should support this migration from one storage protocol to another (ex. FC, iSCSI, NFS, DAS-all of these)
4	Virtualization software shall have High Availability capabilities for the virtual machines in the sense, if in case one server fails all the Virtual machines running on that server shall be automatically restarted on another physical server running same virtualization software. The feature should be independent of Guest Operating System Clustering and withstand multiple host failures with both network and data store heartbeats.
5	Hypervisor platform shall be able to detect the hardware conditions of the host node and shall proactively evacuate the Virtual machines before the hardware issues cause an outage to Virtual machines thus ensuring high availability.
6	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.
7	The solution should support for increasing capacity by adding CPU, Memory or virtual NIC and storage to virtual machines on real time only the fly without any disruption in working or downtime for the virtual machines

Sr. No	Requirement
8	The solution should allow common management across storage tiers and dynamic storage class of service automation via a policy-driven control plane. This is enabled by APIs provided by the Virtualization Solution that enables it to recognize the capabilities of the storage arrays. This insight enables virtualization and storage administrators to automate and easily make decisions.
9	The solution should provide a content library to provide simple and effective centralized management for VM templates, virtual appliances and ISO images. These should be automatically synchronized between multiple virtualization management components at different sites for ease of management
10	Hypervisor shall provide Storage I/O Control for prioritizing storage access by continuously monitoring I/O load of a storage volume and dynamically allocating available I/O resources to virtual machines according to business needs
11	Hypervisor shall provide Network I/O Control for prioritizing network access by continuously monitoring I/O load over the network and dynamically allocating available I/O resources according to business needs.
12	The virtualization platform shall natively provide distributed virtual switch which can span across a virtual datacenter and multiple hosts should be able to connect to it. This in turn will simplify and enhance virtual-machine networking in virtualized environments providing centralized provisioning, administration and monitoring by using cluster level network aggregation.
13	Hypervisor shall provide single Root I/O Virtualization (SR-IOV) Support that allows one PCI Express (PCIe) adapter to be presented as multiple separate logical devices to virtual machines. Let's users offload I/O processing and reduce network latency
14	Hypervisor solution shall provide a framework to deliver proven 3rd party endpoint security solutions to eliminate agent footprint from virtual workloads and offload scanning functions to a security appliance thus reducing impact of security scans on performance by agentless antivirus solution 'deployment.
15	The virtualization software should provide in-built Replication capability which will enable efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
16	Virtualization platform shall have support for Trusted Platform Module (TPM) 2.0 and virtual TPM for enhanced security to protect the hypervisor and guest operating system against unauthorized access
17	Virtualization platform shall have FIPS 140-2 Compliance & TLS 1.2 Support as Default Enhanced security compliance
Management Suite	
1	Virtualization management software console shall provide a single view of all virtual machines, allow monitoring of system availability and performance and automated

Sr. No	Requirement
	notifications with email alerts.
2	The virtualization management software should provide the core administration interface as a single Web based interface. This interface should be flexible and robust and should simplify the hypervisor control through shortcut navigation, custom tagging, enhanced scalability, and the ability to manage from anywhere with Internet Explorer or Firefox-enabled devices.
3	The management software should provide means to perform quick, as-needed deployment of additional hypervisor hosts. This automatic deployment should be able to push out update images, eliminating patching and the need to schedule patch windows.
4	The virtualization should have capability to simplify host deployment and compliance by creating virtual machines from configuration templates.
5	Virtualization management software should have integrated Physical Host and Virtual Machine performance monitoring including CPU, Memory, Disk, Network, Power, Storage Adapter, Storage Path, Cluster services, Virtual machine data stores.
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.
7	Virtualization management software should allow you to deploy and export virtual machines, virtual appliances in Open Virtual Machine Format (OVF).
8	Virtualization management software should allow reliable and non-disruptive migrations for Physical/ Virtual machines running Windows and Linux operating systems to virtual environment.
9	Virtualization management software should include provision for automated host patch management with no VM downtime
10	Virtualization Management console proposed should be able to support up to at least 16 hosts in a single cluster.
11	Virtualization management software should be able to integrate into existing standard EMS systems.
12	The management solution for hypervisor should provide Single-Sign-On capability which should dramatically simplify administration by allowing users to log in once to access all instances or layers of management without the need for further authentication.

Note: Any equivalent open protocols or technical terminologies are allowed.

4.14 Server:

Sr. No	Category	Requirement
1	Form Factor	• 1U/2U Server
2	Processer	• Minimum Dual 64-Core, latest series/generation, Intel® Xeon® or AMD scalable processors, with 2.4 Gbhz or more base frequency
3	Motherboard	• OEM Supported Mother Board and Chipset
4	System Memory	• Min 768 GB DDR-5 or Latest, supported up to 4 TB or higher with 24 or more DIMM slots; ECC Advance
5	Disks supported	• 2.5" Hard Drives bay (HDD/SSD),
6	RAID Controller	• 4 Gbps PCIe 3.0 with RAID 5/6 or better
7	Disks configured	• 2*480GB NVMe SSD , 2.5in Hot-plugin, support up to 8 drives
8	Network Interface	• On-Board management port
		• 2 x Dual Port 10/25G Network Card
		• infiniband Options Support for future • expansions: 100Gb or 200Gb Single or Dual port Adapter
9	HBA Card	• 64 Gbps Host Bus Adaptor for connecting to SAN Switch with Storage.
10	Interface	• Serial Port, 2 x USB 3.2 Gen 1Port,
11	Certification and compliances	• Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Microsoft Windows Server
12	Power Supply	• Appropriate energy efficient redundant
13	Management integration	• Support for integration with VMware vCenter
14	Management Features-1	• Remoter power On/ Shutdown of server, • Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port, • Should have virtual Media support with all required licenses., • Remote KVM, Server Health Logging, Out of Band Management
15	Management Features-2	• Management of multiple Servers from single console with single source of truth for multiple sites., • Automated infrastructure management for patch upgrades, version upgrades, etc. • Simplified management with analytics driven actionable intelligence., • System tagging giving admin flexibility to provide metadata tags to each

Sr. No	Category	Requirement
		System to enable users to filter and sort systems based on user-assigned attributes, • Platform inventory and health status, Server utilization statistics collection (including firmware updates and diagnostic tools), Should provide an alert in case the system is not part of OEM hardware compatibility test, • Should have customizable dashboard to show overall faults/health/inventory for all managed infrastructure the solution • Real-time out-of-band hardware performance monitoring & alerting, • The Infrastructure Management solution quoted should provide some level of call home capability to readily identify any hardware issues in the environment to enable higher availability of services. The Infrastructure Management solution quoted should provide some level of call home capability to readily identify any hardware issues in the environment to enable higher availability of services. The Infrastructure Management solution quoted should have the capability to integrate with Log Analytics solution. • The Infrastructure Management solution quoted should have the capability to integrate with Log Analytics solution.
16	Security Features-1	• For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint.
17	Security Features-2	• Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.
18	Industry Standard Compliance	• ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3, TLS 1.2, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4. Or any equivalent.
19	System Security	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms

Sr. No	Category	Requirement
		(CNSA), Chassis Intrusion detection option
20	Support for high availability clustering and virtualization	Yes
21	Implementation Services and On-Site Comprehensive Warranty Support directly from OEM	• Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 +3 years 24 x 7 Proactive warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider or any other agency during the entire contract duration of 7 +3 years.

Note: Any equivalent open protocols or technical terminologies are allowed.

4.15 Enterprise Storage:

Sr. No	Category	Requirement
1	Platform	• Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives. • The storage should have Symmetric/Asymmetric Active-Active Controller architecture • The proposed Storage model must support scaling-up or scaling-out to at least 8-Controllers either on common backplane or federation.
2	Hypervisor Support	• Offered platform shall provide the simplicity of converged storage from a well- known Hypervisor like VMware / Microsoft / Linux Platform along with required licenses as per below specifications and requirements.
3	Capacity & Scalability	• 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.

Sr. No	Category	Requirement
4	Cache	• 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. • Write operations shall be completely protected and there shall be no data loss in case of power failure. This mechanism must not rely on external batteries.
5	No Single point of Failure & Performance	• Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc. • There shall be no/minimal performance de-gradation due to a single component or controller failure.
6	Disk Drive Support and Encryption	• Offered Storage array shall support various capacities of NVMe flash and NL-SAS drives. • The proposed storage must support data encryption with day 1.
7	Data Tiering	• Offered Storage array shall be able to tier NVMe SSD and SAS/NL-SAS Drives in a single pool.
8	RAID Support	• Offered Storage array shall be provided with two drive or better failure protection simultaneously.
10	Availability	• Offered platform shall be configured in no single point of failure-environment. Vendor shall design in such a way that storage layer shall provide 99.9999% data availability. • The storage must provide non-disruptive firmware/micro code upgrade, logical device reallocation and configuration changes.
11	Global Hot Spare	• Offered Storage Array shall support distributed Global Hot Spare for offered Disk drives. • Global hot spare shall be configure as per industry practice.
12	Integration VMWARE Integration	• Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL. • Shall be certified for vVol based replication. • Shall support both compression and de-duplication. • Shall be qualified to work with both Fibre Channel • Shall support Scheduled snapshot and quality of service. • Shall support encryption.
13	Storage Management Features	• Centralized Storage management software should be browser based/ web enabled accessible over IP • Storage management software should have roles based access for user accounts to manage and monitor the storage system

Sr. No	Category	Requirement
		• Storage management software should be able to integrate with Active Directory/ LDAP for user authentication • Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API • Storage management software should provide simplified user interface and wizards to perform configuration operations like create LUNs, Pools, Tiers, present LUNs to host, etc. • Storage management software should be able to Orchestrate and Automate storage configuration operations • Storage management software should be able to Automate Replication Operations and monitor local and remote replication operations including 3DC or Active-Active Storage replication • Storage Management software should be able to define storage-centric data replication policies and automate the storage-based replications • Storage management software should be able to monitor alerts for automated or manually set performance thresholds. • Storage management software should be able to generate trending, Predictive Analysis, forecasting of Performance and Capacity of the complete Storage Infrastructure • Storage management software should be able to identify performance bottleneck, Root Cause Analysis at host, SAN and storage level and should be able to troubleshoot storage performance problems
15	Quality of service	• The storage should be able to provide Quality or Service (QOS) to ensure bandwidth is allocated to desired servers or ports, storage should be capable of restricting IOs or throughput to LUNs or Volmes.
16	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.
17	Thin Provisioning and Space optimization	• Offered platform shall support critical global data efficiency features - inline de-duplication, inline compression and thin provisioning.
18	Snapshot / Point in time copy / Zero Copy Clone / Thin Clone	• The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 500, total system should support at least 50,000 snapshots. Minimum 6 clone copies of each lun should be supported. • The storage should be supplied with Storage management, virtual/thin provisioning, snapshot, clone, Sub-Lun Data Tiering and other

Sr. No	Category	Requirement
		required software to meet the technical requirements. Licenses to be supplied for Unlimited capacity.
19	Remote Replication	• The storage should support both Synchronous and Asynchronous Data Replication to remote site. The Storage should also capable of supporting 3-Way Disaster Recovery with Zero Data Loss Delta Resync. • 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.
20	Licenses	• Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, Remote replication, QOS etc. for the maximum supported capacity of platform. There shall be no additional software license requirement for future capacity upgrade. Any additional license required for meeting the RFP specification shall also be offered upfront.
21	Implementation Services and On-Site Comprehensive Warranty Support directly from OEM	• Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7 years+ 3 year extendable 24 x 7 warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider during the entire warranty duration of 7+3 years extendable. • TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR
22	Data Loss	• The solutions should ensure zero data loss (OEM need to provide assurance in the MAF)

Note : Any equivalent open protocols or technical terminologies are allowed.

4.16 Backup Storage:

Sr. No	Category	Requirement
1	Platform	• Offered Storage array shall be a true flash optimized Hybrid array supporting both SSD NVMe drives and spinning drives. • The storage should have Symmetric/Asymmetric Active-Active Controller architecture
2	Hypervisor Support	• Offered platform shall provide the simplicity of converged storage from a well- known Hypervisor like VMware / Microsoft / Linux Platform along with required licenses as per below specifications and requirements.

Sr. No	Category	Requirement
3	Capacity & Scalability	• The Storage Array shall be offered with 220TiB (BASE-2) without Dedupe and compression in RAID6 or better configuration Offered storage array shall be flexible on both Scale-up and Scale-out using array in-built firmware enabled clustering technology.
4	Cache	• The storage system should have minimum 256 GB 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. • Write operations shall be completely protected and there shall be no data loss in case of power failure. This mechanism must not rely on external batteries.
5	No Single point of Failure & Performance	• Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc. • There shall be no/minimal performance de-gradation due to a single component or controller failure.
6	Disk Drive Support	• Offered Storage array shall support various capacities of NL-SAS drives.
7	Data Tiering	• Offered Storage array shall be able to tier NVMe SSD and SAS/NL-SAS Drives in a single pool for optimizing performance if required.
8	RAID Support	• Offered Storage array shall be provided with two drive or better failure protection simultaneously.
10	Availability	• Offered platform shall be configured in no single point of failure-environment. Vendor shall design in such a way that storage layer shall provide 99.9999% data availability. • The storage must provide non-disruptive firmware/micro code upgrade, logical device reallocation and configuration changes.
11	Global Hot Spare	• Offered Storage Array shall support distributed Global Hot Spare for offered Disk drives. • Global hot spare shall be configure as per industry practice.
12	Integration - VMWARE vVol Integration	• Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL. a) Shall be certified for vVol based replication. b) Shall support both compression and de-duplication. c) Shall be qualified to work with both Fibre Channel and ISCSI. d) Shall support Scheduled snapshot and quality of service. e) Shall support encryption.

Sr. No	Category	Requirement
13	Storage Management Features	• Centralized Storage management software should be browser based/ web enabled accessible over IP • Storage management software should have roles based access for user accounts to manage and monitor the storage system • Storage management software should be able to integrate with Active Directory/ LDAP for user authentication • Storage management software should be able to integrate with 3rd party enterprise management system via RESTFul API • Storage management software should provide simplified user interface and wizards to perform configuration operations like create LUNs, Pools, Tiers, present LUNs to host, etc. • Storage management software should be able to Orchestrate and Automate storage configuration operations • Storage management software should be able to Automate Replication Operations and monitor local and remote replication operations including 3DC or Active-Active Storage replication • Storage Management software should be able to define storage-centric data replication policies and automate the storage-based replications • Storage management software should be able to monitor alerts for automated or manually set performance thresholds • Storage management software should be able to generate trending, Predictive Analysis, forecasting of Performance and Capacity of the complete Storage Infrastructure • Storage management software should be able to identify performance bottleneck, Root Cause Analysis at host, SAN and storage level and should be able to troubleshoot storage performance problems
15	Quality of service	• The storage should be able to provide Quality or Service (QOS) to ensure bandwidth is allocated to desired servers or ports, storage should be capable of restricting IOs or throughput to LUNs or Volmes.
16	Host Ports	• Offered Storage array shall be supplied with at-least dual controllers and 8 x 32 Gbps FC ports across controllers. All offered card shall be capable to work at line speeds.
17	Thin Provisioning and Space optimization	• Offered platform shall support critical global data efficiency features – inline / post de-duplication, inline /POST compression and thin provisioning.

Sr. No	Category	Requirement
18	Snapshot / Point in time copy / Zero Copy Clone / Thin Clone	• The storage should support in-system replication such as snapshots and clones. Minimum number of snapshots for each Lun should be at least 500, total system should support at least 50,000 snapshots. Minimum 6 clone copies of each lun should be supported. • The storage should 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.
19	Licenses	• Vendor shall provide the license for all critical functionalities like capacity expansion, Snapshot, Thin Clone, 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.
20	Implementation Services and On-Site Comprehensive Warranty Support directly from OEM	• Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. The engineers must be on OEM company payroll. Similarly, comprehensive 7+3 extendable years 24 x 7 warranty services shall be rendered directly by OEM resources only and must not be offloaded to partner or service provider during the entire warranty duration of 7 + 3 years extendable. • TEC/GR/IT/DSI-001/04/DEC 2015 or latest Tech GR

Note : Any equivalent open protocols or technical terminologies are allowed.

4.17 Backup Server:

Sr. No	Category	Requirement
1	Chassis	• 1U/2U rack mountable with 19" industry standard rail-kit
2	CPU	• 1 x 16-core latest generation Intel/AMD processor, minimum 2.7 GHz with a boost of 4.1 GHz or higher, 60MB or more cache
3	Memory	• 128GB DDR5 memory, scalable upto 4TB or higher with 24 or more DIMM slots
4	HDD	• 2 x 1.92TB NVMe SSD with RAID 1
5	Networking	• 2 x dual port 10/25Gbps SFP28 adapters with transceiver modules
6	Infiniband Networking	• Infiniband Options Support for future expansions: 100Gb or 200Gb Single or Dual port Adapter
7	Fiber Channel	• 2 x 32Gbps FC ports
8	Interfaces	• 2 x USB 3.2 Gen1 ports or higher

Sr. No	Category	Requirement
9	Bus Slots	• 4 x PCIe 5.0 or higher slots
10	Power Supply	• Support for 2 x 1600W or higher 80PLUS Platinum hot-plug redundant power supply
11	Fans	• Redundant hot-plug system fans
12	Industry Standard Compliance	• ACPI 6.1 Compliant, PCIe 5.0 Compliant, WOL Support, Microsoft® Logo certifications, PXE Support, Energy Star, SMBIOS 3.1, UEFI 2.9, Redfish API, IPMI 2.0, Secure Digital 2.0, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), SNMP v3 TLS 1.2, DMTF Systems Management Architecture for Server, Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0, ASHRAE A3/A4
13	System Security	• UEFI Secure Boot and Secure Start support, Tamper-free updates - components digitally signed and verified, Common Criteria certification, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms (CNSA), Chassis Intrusion detection option
14	Operating Systems and Virtualization Software Support	• Offered server must support Red Hat Enterprise Linux 8.6 or higher, Vmware 8.0 or higher
15	Firmware security	• For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. • Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.
16	Embedded Remote Management and firmware security	• System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder. • Server should have dedicated 1Gbps remote management port • Server should support storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to

Sr. No	Category	Requirement
		rollback/patch faulty firmware. • 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.
17	Management	• The Infrastructure Management solution quoted should provide some level of call home capability to readily identify any hardware issues in the environment to enable higher availability of services.
		• The Infrastructure Management solution quoted should have the capability to integrate with Log Analytics solution.
		• Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
		• The Systems Management software should provide Role-based access control.
18	Warranty	• 10 year (7 by OEM +3 extendable years by Bidder) 24x7 comprehensive warranty from the server OEM from day one.
19	Implementation Services and On-Site Comprehensive Warranty Support directly from OEM	• Complete configuration and end-to-end implementation & commissioning services shall be directly rendered and delivered by OEM engineers directly. Similarly, comprehensive 7+3 extendable 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

Note : Any equivalent open protocols or technical terminologies are allowed.

4.18 Backup Software:

Sr. No	Category	Requirement
1	Licensing	• The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary 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/Container workloads; without the need of a 3rd party solution.
2	Reporting Capabilities	• Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied. • Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts. • Proposed solution should have security and compliance dashboard inbuilt with the product. • Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
4	Security &Compliance	• The backup software must have YARA rules defined in the system. • The proposed solution should have on demand scans available for malware attacks. • The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks. • The proposed backup software should have four eyes approval for any backup deletion.

Sr. No	Category	Requirement
5	Backup support for hypervisors and Applications	• Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention. • 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 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 console auto log-off functionality.
6	RPO/ RTO and Recovery Assurance	• Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability. • Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, 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 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.

Sr. No	Category	Requirement
7	Backup and Replication Performance and SLA	• The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads. • Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO. • The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.
8	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 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 of workloads between dis-similar systems like hyper converged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. • Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the dissimilar hardware.
9	Warranty	• 7+3 extendable years 24x7 comprehensive warranty from the server OEM from day one.

4.19 End point Protection of VMs:

Sr. No	Category	Requirement
1	Functionality	• 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.

Sr. No	Category	Requirement
		• Supports Ipv4 and Ipv6 • Comprehensive protection against viruses, Trojans, worms, spyware, adware, and other malicious tools. • Full malware scan with configurable exclusions and performance controls • Utilizes behaviour monitoring and machine learning to detect file less attacks and unknown threats with an in-house anti-malware engine • Safeguards documents from ransomware • Should support detection of all types of malware (known & unknown) • Blocks Command and Control (C&C) traffic, malicious websites, and protects against vulnerabilities and CVE-based rules. • Asked requirements shall be provided to compute and storage setup.

Note : Any equivalent open protocols or technical terminologies are allowed.

4.20 Network Time Protocol (NTP):

Sr. No	Requirement
1	• The device shall support NTP packets with a total of 140,000 NTP transactions per second including MD5 or better security/encryption, The device shall allow the use GNSS with Multiband as a source of time, The device shall allow support ePRTC mode for NTP (with additional caesium), NTP and SyncE to be used on the same Ethernet port, NTP services on ports supporting Fast Ethernet, 1Gb.
2	• The Device shall be able to support NTP and G.8275.1 on the same Ethernet port, 2 devices may be used as a redundant pair, in 1:1 protection mode. The device shall be configured via CLI over SSH, not use or support telnet or FTP for security reasons. Web interface using HTTPs for performance monitoring, have 10Mhz and 1pps outputs for verification purposes, The Device shall have up to 4 x E1 outputs for future use. The Device shall accept have 2 PPS-TOD ports where each one can be configured for input or output, accept a PTP input, to be used as a primary or backup input for GNSS, The device shall use phase based APTS for the backup PTP input. • TEC 48150:2024

4.21 DHCP-DNS-IPAM Solution:

Sr. No	Requirement
1	• DDI System must be an Hardware Appliance based solution providing DNS, DHCP & IPAM Service with defined features & capacity. The bidder may purposed software based solutions with equivalence of functional specification.

Sr. No	Requirement
2	• DDI System must provide integrated support for high availability configurations without the requirement for licensing of additional third -software components.
3	• DDI System must support System logs forwarding/redirection of logs to a defined syslog host.
4	• DDI system must support monitoring using SNMPv3
5	• DDI system must support NTP time synchronization (client-mode) to multiple servers.
6	• DDI system must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory
7	• DDI Solution must support GUI & CLI based configuration.
8	• DDI Solution must have DNS, DHCP & IPAM solution be integrated together
9	• DDI Hardware Appliance should have Dual Power supply.
DDI Specific Requirements	
I	**IPAM**
1	• The IPAM Solution must support all the IP Address Management for both IPv4 & IPv6 together on the same proposed IPAM Hardware Appliance. • The bidder may purposed software based solutions with equivalence of functional specification.
2	• The solution must NOT use software agents or thick clients
3	• The IPAM solution must provide high-availability at DC
4	• System proposed should be deployed 1 Qty at DC & 1 Qty at DR as dedicated IPAM Server.
5	• The solution should provide appropriate automated failover without any manual intervention.
6	• The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.
7	• The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.
8	• The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records
9	• The IPAM solution should be able act as Central management Server for proposed DNS & DHCP Server from single vendor & should have inbuilt reporting for IPAM Appliance for proposed DDI Solution.

Sr. No	Requirement
10	• The IPAM solution should be able to create its own widget to display customized subnet reports, free IP, used IP.
11	• The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network.
12	• DDI IPAM user interface must be web-based without specific browser vendor requirements
13	• DDI IPAM system should support Auto seamless failover within DC
14	• DDI IPAM system should support VLSM (Variable Length Subnet Masks)
15	• DDI IPAM system should be able to export reports in PDF, CSV format
16	• DDI IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability.
17	• DDI audit records should contain a timestamp, username and record modified.
18	• DDI Reporting engine should include audit reports.
19	• DDI system should support granular rights administration limiting the function and rights to user and Subnet level
20	• The tool must have the capability to find free address space across a range
23	• The IPAM Solution Component must discovery 200 Cloud Instances running on Amazon AWS, Google GCP & Microsoft Azure and Virtual Instance running on Vmware VCenter
II	**Internal DNS & DHCP Server**
1	• Solution should support standards-based Internal DNS & DHCP services.
2	• The solution should support the ability to act as an Internal Cache, Recursive & Authorative nameserver
3	• System proposed should be deployed 2 Qty at DC & 2 Qty at DR as dedicated Internal DNS & DHCP Hardware Appliance • The bidder may purposed software based solutions with equivalence of functional specification.
4	• The Solution should support 25,000 DNS QPS acting as Internal Authoritative DNS Server
5	• The solution must be able to handle 400 DHCP Lease/sec
5	• The Solution Should support to configure 50 Zone.
6	• The Solution Should support to configure 10000 record

Sr. No	Requirement
7	• The Solution should support Master-Slave, Multi Master or Stealth Mode deployment architecture.
8	• The solution should be able to automate common tasks such as maintaining synchronization between forward and reverse records
9	• Authoritative Name Servers should have the built-in protection using Response Rate limiting
10	• The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)
11	• The Solution should support A, NAPTR, SRV, NS, MX, CNAME records
12	• Should support IPv6 : AAAA, PTR, host, ip6.arpa, DDNS records
13	• Solution should support multiple DNS views based on IPv4/Ipv6 Addresses
14	• The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc
15	• The solution should support easy search, sort and filter on any DNS Zone or RR, using any field
16	• The product must support the ability to control DNS logging : DNS query and response logging
17	• The solution should provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.
18	• The system should be able to display all hosted DNS Resource Records in one GUI pane
19	• Import Wizard solution must be built-in solution by the DNS Appliance and must not require any external Java program or external Virtual Machines
20	• The solution should provide a means to track changes to made via Dynamic DNS record assignment
21	• The solution must support the standard DNSSEC specifications for serving of DNSSEC signed zones and the pass-through of client resolution of external zones
22	• The solution must support secure dynamic updates from Microsoft clients using the Microsoft Generic Security Service Transaction Signature (GSS-TSIG) standard
23	• The solution must support TSIG for authentication of zone transfers and dynamic updates
24	• The solution must have in build reports & Stats.
25	• The solution must provide an easy to use "import wizard" to import DHCP records from legacy DHCP Solution

Sr. No	Requirement
26	• Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines
28	• The DHCP solution must provide high-availability
29	• The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making the change, and a timestamp. The solution should also be able to identify the client IP address from where the change was made.
31	• The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.
32	• The solution must graph (visually display) the different scopes based on number of IP's used/available over a set period of time
33	• The DHCP solution must support one IP per MAC address (one lease per client).
34	• The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP
35	• The solution must provide device finger printing and display or report the data in the GUI
36	• The solution must support creating DHCP custom options.
37	• The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc
38	• The DHCP Solution must integrate to IPAM for lease consolidation and capacity planning
39	• The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses
40	• The DHCP Solution must be able to send alerts in case of DHCP related attacks
41	• The DHCP Solution must have inbuilt Reports & stats.

Note: Any equivalent open protocols or technical terminologies are allowed.

4.22 Syslog Server:

Sr. No	Category	Requirement
1	Centralized Log Management	• Provides a centralized solution for collecting, analysing, and forwarding logs in real-time.
2	Log Sources	• Supports Syslog messages and SNMP traps and any type from network

Sr. No	Category	Requirement
		devices (routers, switches, firewalls) and host OS.
3	Web Console	• Includes an intuitive web-based console to view, search, and filter syslog messages with up to 10 customizable views.
4	Filtering & Search	• Allows filtering based on time, hostname, severity, and custom alerts for proactive log management.
5	Graphical Insights	• Generates visual graphs for syslog statistics over specific time periods.
6	Alert Mechanism	• Supports email alerts, instant messaging, sound alerts, SMS, and automated responses based on predefined log criteria.
7	Compliance & Archival	• Supports scheduled log archival, clean-up, and regulatory compliance with SOX, PCI-DSS, FISMA.
8	Security & Access Control	• Role-based access control (RBAC) for user permissions; manages audit logs for accountability.
9	Scalability	• Designed to handle a large volume of messages per hour; supports both IPv4 and IPv6 devices. Offered product should support DC/DR architecture.
10	Integration	• Can forward syslog messages and SNMP traps (v1, v2, v3) to external hosts and integrate with external network management systems.
11	Automation	• Allows execution of scripts or external programs based on log triggers; supports automated log compression, encryption, and deletion.
12	Device & User Management	• Provides device grouping, user role management, department-wise access configuration, and location-based log categorization.
13	Storage & Retention	• Supports log storage in files, databases, and ODBC-compliant databases with configurable retention policies.
14	Certification	• Offered product should be Trusted Telecom approved. Supporting certificate/approval required.

Note : Any equivalent open protocols or technical terminologies are allowed.

SECTION-5 INSTRUCTIONS TO BIDDERS

5.1 General Instruction to Bidders

All information supplied by Bidders may be treated as contractually binding on the Bidders on successful award of the assignment by the TENDERER on the basis of this RFP. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the TENDERER. Any notification of preferred bidder status by the TENDERER shall not give rise to any enforceable rights by the Bidder. The TENDERER may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the TENDERER.

This RFP supersedes and replaces any previous public documentation, communications, and Bidders should place no reliance on such communications. The TENDERER may terminate the RFP process at any time and without assigning any reason. The TENDERER makes no commitments, express or implied, that this process will result in a business transaction with anyone. Bidder cannot participate the

5.2 Cost of Bidding

- The Bidder shall bear all costs associated with the preparation and submission of the Bid. The TENDERER will in no case be responsible for those costs, regardless of the conduct or outcome of the bidding process.
- Cost of tender document (Tender fee, if applicable) is non-refundable and cannot be exempted in any condition.
- In case of non-receipt of EMD within stipulated timeline, the bid will be rejected by GFGNL/Dept. of Science & Technology as non-responsive.

5.3 Bidding Document

Bidder can download the bid document and further amendment if any freely available on https://bharatnet.gujarat.gov.in/ and eProc-Suite (nprocure.com) and upload the same on eProc-Suite (nprocure.com) on or before due date of the tender. Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submits a Bid not substantially responsive to the bidding documents in every respect may result in the rejection of the Bid. Under no circumstances physical bid will be accepted.

5.4 Clarification on Bidding Document

Bidders can seek written clarifications by submit its queries, via email to below mail-ids on or before the last date of sending queries as defined in this document.

dgmnoc-gfgnl@bharatnet.gujarat.gov.in,
pmc2@bharatnet.gujarat.gov.in
pmc3@bharatnet.gujarat.gov.in,
pmc@bharatnet.gujarat.gov.in,

The queries should necessarily be submitted with below format in Microsoft Excel (*.xls or *.xlsx) only.

Sr.	Page no	Clause/ Sub-clause no	Content of the RFP Requiring Clarification	Clarification Sought	Justification

GFGNL will host a Pre-Bid meeting on the date defined in this document to address the queries (if any) by prospective bidders and may clarify their doubts or share any additional information necessary for them to submit their bid successfully. The representatives of the bidders may attend the Pre-Bid Meeting at their own cost.

A constituent of the GFGNL PH-III (ABP- Amendment Bharatnet program) RFP or Such Bidder has the same authorized representative for purposes of this Bid as any other Bidder for the same RFP

For the same Package, such Bidder, or any Associate thereof has participated as a consultant to GFGNL in the preparation of any documents, design or technical specifications of the Package.

5.5 Amendment of Bidding Documents

At any time prior to the deadline for submission of bids, the TENDERER, for any reason, whether at its own initiative or in response to the clarifications requested by prospective bidders may modify the bidding documents by amendment & put on our websites.

All prospective bidders are requested to browse TENDERER'S website & any amendments/ corrigendum/ modification will be notified on the website and such modification will be part of RFP and binding on them.

To allow prospective bidders a reasonable time to take the amendment into account in preparing their bids, the TENDERER, at its discretion, may extend the deadline for the submission of bids.

5.6 Language of Bid

The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the TENDERER shall be in English.

5.7 Bid Security/ Earnest Money Deposit (EMD)

- Bidders shall submit, along with their Bids, Rs.1,00,00,000/- (Rupees One Crore only) in the form of an unconditional Bank Guarantee by Bank Guarantee (which should be valid for 6 months from the last date of bid submission) of any Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative Banks and Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. No. EMD/10/2020/42/DMO dated 19.10.2020 , GR. No.: FD/MSM/e-file/4/2023/4020/D.M.O. 21/04/2023 issued by Finance Department or further instruction issued by Finance department

time to time; in the name of “Gujarat Fibre Grid Network Limited.” Payable at Gandhinagar (in the specified format and must be submitted along with the covering letter.

- EMD of all unsuccessful bidders would be refunded by GFGNL within 60 Days on selection of successful bidder.
- The EMD of the successful bidder would be returned upon successful submission of Performance Bank Guarantee as per the provided format.
- EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.
- The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.
- The EMD may be forfeited, In case of a Bidder if:
  - The bidder withdraws its bid during the period of bid validity.
  - The Bidder does not respond to requests for clarification of their Bid.
  - The Bidder fails to cooperate in the Bid evaluation process.
  - In case of successful bidder, the said bidder fails:
    - Fails to sign the agreement in time.
    - Fails to submit performance bank guarantee.

5.8 Late Bids

- Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall be REJECTED.
- The bids submitted by telex/telegram/ fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

5.9 Section Comprising the Bids

- All forms / Tables, duly filled-in with necessary proofs, as required and stated in the bid document & supporting documents for eligibility criteria should be uploaded. The bid uploaded shall have the following documents:
  - BID SECURITY SECTION

    The bid security in the form of EMD to be prepared preferable in the form of demand draft (or through digital transfer) in favor of “Gujarat Fibre Grid Network Limited.” Payable at Ahmedabad/ Gandhinagar before the last date and time of the bid submission.

    The copy of EMD is to be uploaded on procure portal along with the bid on or before the bid submission date. For the confidentiality, the bidder is allowed to submit original EMD (proof of transaction receipt) at correspondence office within 4 working days after the bid submission date.

    ELIGIBILITY SECTION

All relevant documents mentioned in eligibility criteria.

- **PRICE BID** SECTION

Priced bid (in the prescribed format)

Note: Filling up prices anywhere other than the prescribed shall render the bidder disqualified.

- **Annexures &** Formats
- Wherever a specific form is prescribed in the Bid document, the Bidder shall use the form to provide relevant information. If the form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information. Failing to submit the information in the prescribed format, the bid is liable for rejection.
- For all other cases, the Bidder shall design a form to hold the required information.
- TENDERER shall not be bound by any printed conditions or provisions in the Bidder's Bid Forms.
- The prices shall strictly be submitted in the given format. Successful Bidder will have to supply/ provide Services with an Invoice from a place located within State of Gujarat.
- Prices shall be written in both words and figures. In the event of difference, the price in words shall be valid and binding.
- Offered price should be inclusive of all applicable taxes (anywhere in Gujarat state).

5.10 Bid Opening

- Bids will be opened in the presence of Bidder's representatives, who choose to attend. The Bidder's representatives who are present shall sign a register evidencing their attendance.
- In the event of the specified date of Bid opening being declared a holiday for the GFGNL, the Bids shall be opened at the appointed time and location on the next working day.
- The Bidder's names, bid modifications or withdrawals, discounts and the presence or absence of relevant Bid security and such other details as the TENDERER officer at his/her discretion, may consider appropriate, will be announced at the opening.
- Immediately after the closing time, the TENDERER contact person shall open the Un-Priced Bids and list them for further evaluation.
- Bids that are not opened at bid opening shall not be considered further for evaluation.

5.11 Bid Validity

- Bids shall remain valid for 180 days after the date of Bid opening prescribed by the TENDERER. A Bid valid for a shorter period shall be rejected as non-responsive. In

exceptional circumstances, the TENDERER may solicit Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The Bid security shall also be suitably extended. A Bidder's request to modify the Bid will not be permitted.

5.12 Contacting the Tenderer

Bidder shall not approach the TENDERER officers outside of office hours and/ or outside the TENDERER office Premises, from the time of the Bid opening to the time the Contract is awarded. Any effort by a bidder to influence the TENDERER officers in the decisions on Bid evaluation, bid comparison or contract award may result in rejection of the Bidder's offer. If the Bidder wishes to bring additional information to the notice of the TENDERER, it should do so in writing.

5.13 Rejection of Bids

The TENDERER reserves the right to reject any Bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for such decision.

5.14 Bid Evaluation Process

- The TENDERER will form a committee which will evaluate the proposals submitted by the bidders for a detailed scrutiny. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarification of their Proposals.
- The bidders are expected to provide all the required supporting documents & compliances as mentioned in this RFP.
- During the evaluation, committee may seek the clarification in writing from the bidder, if required. If bidder fails to submit the required clarifications in due time, the evaluation will be done based on the information submitted in the bid.

5.15 Award of Contract

As per QCBS method.

5.16 Notification of Award & Signing of Contract

- Prior to expiration of the period of Bid validity, the TENDERER will notify the successful Bidders and issue LoI.
- Within two weeks of receipt of the Contract form, the successful bidder shall sign and stamp the contract and return it to the TENDERER along with performance guarantee.

5.17 Force Majeure

Force Majeure shall mean any event or circumstances or combination of events or

circumstances that materially and adversely affects, prevents or delays any Party in performance of its obligation in accordance with the terms of the Agreement, but only if and to the extent that such events and circumstances are not within the affected party's reasonable control, directly or indirectly, and effects of which could have prevented through Good Industry Practice or, in the case if construction activities through reasonable skill and care, including through the expenditure of reasonable sums of money. Any events or circumstances meeting the description of the Force Majeure which have same effect upon the performance of any contractor shall constitute Force Majeure with respect to the bidder. The Parties shall ensure compliance of the terms of the Agreement unless affected by the Force Majeure Events. The bidder shall not be liable for forfeiture of its implementation / Performance guarantee, levy of Penalties, or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Agreement is the result of Force Majeure.

5.18 Force Majeure Events

The Force Majeure circumstances and events shall include the following events to the extent that such events or their consequences (it being understood that if a causing event is within the reasonable control of the affected party, the direct consequences shall also be deemed to be within such party's reasonable control) satisfy the definition as stated above. Without limitation to the generality of the foregoing, Force Majeure Event shall include following events and circumstances and their effects to the extent that they, or their effects, satisfy the above requirements:

- **Natural events** ("Natural Events") to the extent they satisfy the foregoing requirements including:
  - Any material effect on the natural elements, including lightning, fire, earthquake, cyclone, flood, storm, tornado, or typhoon.
  - Explosion or chemical contamination (other than resulting from an act of war);
  - Epidemic such as plague.
  - Any event or circumstance of a nature analogous to any of the foregoing.
- Other Events ("Political Events") to the extent that they satisfy the foregoing requirements including:
  - Political Events which occur inside or Outside the State of Gujarat or involve directly the State Government and the Central Government ("Direct Political Event"), including:
  - Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act of terrorism or sabotage.
  - Strikes, work to rules, go-slows which are either widespread, nation- wide, or state-wide or are of political nature.
  - Any event or circumstance of a nature analogous to any of the foregoing.

- **Force majeure** exclusions:

  Force Majeure shall not include the following event(s) and/or circumstances, except to the extent that they are consequences of an event of Force Majeure:

  - Unavailability, late delivery
  - Delay in the performance of any contractor, sub-contractors or their agents.

- **Procedure for calling force** majeure:

  The Affected Party shall notify to the other Party in writing of the occurrence of the Force Majeure as soon as reasonably practicable, and in any event within 05 (five) days after the Affected Party came to know or ought reasonably to have known, of its occurrence and that the Force Majeure would be likely to have a material impact on the performance of its obligations under the Agreement.

5.19 Contract Obligations

Once a contract is confirmed and signed, the terms and conditions contained therein shall take precedence over the Bidder's bid and all previous correspondence.

5.20 Insurance

Without limiting any of his other obligations or liabilities, the bidder shall, at his own expense, take and keep comprehensive insurance including third party risk for the plant, machinery, men, materials etc. brought to the site and for all the work during the execution and Operation & Maintenance. The bidder shall also take out workmen's compensations insurance as required by law and undertake to indemnify and keep indemnified GFGNL from and against all manner of claims and demands and losses and damages and cost (including between attorney and client) charges and expenses that may arise in regard the same or that USOF, DoT/ GFGNL may suffer or incur with respect to end / or incidental to the same. The bidder shall have to furnish originals and/or attested copies as required by the department of the policies of insurance taken within 15 (fifteen) days of being called upon to do so together with all premium receipts and other papers related thereto which USOF, DoT/ GFGNL may require.

The bidder shall insure all the equipment at site for theft, damages due to fire, flood, earthquake, storm etc for the entire project duration

5.21 Amendment to the Agreement

Amendments to the Agreement may be made by mutual agreement by both the Parties. No variation in or modification in the terms of the Agreement shall be made except by written amendment Signed by both the parties. All alterations and changes in the Agreement will consider prevailing rules, regulations and laws applicable in the state of Gujarat.

5.22 Representations and Warranties

- Representations and Warranties by the Selected Agency**:**

- It is a company duly organized and validly existing under the laws of India and has all requisite legal power and authority and corporate authorizations to execute the Agreement and carry out the terms, conditions and provisions hereof. It has in full force and effect all requisite clearances, approvals and permits necessary to enter into the Agreement and perform its obligations hereof.
- The Agreement and the transactions and obligations hereof do not contravene its constitutional documents or any law, regulation or government directive and will not contravene any provisions of, or constitute a default under, any other Agreement or instrument to which it is a party or by which it or its property may be bound or any of its obligations or undertakings by which it or any of its assets are bound or cause a limitation on its powers or cause it to exceed its authorized powers.
- Bidder nor any of its affiliates have immunity from the jurisdiction of a court of from legal process (whether through service of notice, attachment prior to judgement), attachment in aid of execution or otherwise). The successful bidder confirms that all representation and warrantied of the bidder set forth in the Agreement are true, complete in all respects.
- No information given by the Successful Bidder in relation to the agreement, project documents or any document comprising security contains any material wrong statement of fact or omits to state as fact which would be materially averse to the enforcement of the rights and remedies of TENDERER or which would be necessary to make any statement, representation or warranty contained herein or therein true and correct.
- Representations and Warranties by the TENDERER
- It has full legal right; power and authority to execute the said project and to enter into and perform its obligations under the Agreement and there are no proceedings pending.
- The Agreement has been duly authorized, executed and delivered by the TENDERER and constitutes valid, legal and binding obligation of TENDERER.
- The execution and delivery of the Agreement with the selected agency does not violate any statutory judgment, order, decree, regulation, right, obligation or rule of any court, government authority or arbitrator of competent jurisdiction applicable in relation to the TENDERER, its assets or its administration.

5.23 Resolution of Disputes

- If any dispute arises between the Parties hereto during the subsistence or thereafter, in connection with the validity, interpretation, implementation or alleged material breach of any provision of the Agreement or regarding a question, including the questions as to whether the termination of the Contract Agreement by one Party hereto has been legitimate, both Parties hereto shall endeavor to settle such dispute

amicably. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts [which attempt shall continue for not less than 30 (thirty) days], give 15 days' notice thereof to the other Party in writing. The said clause shall not be applicable in the case of cyber-crimes and any other type of security breach relating to PHI carried out by either bidder organization itself or its employees.

- In the case dispute arising between the parties in the contract, which has not been settled amicably, any party can refer the dispute for Arbitration under (Indian) Arbitration and Conciliation Act, 1996. Such disputes shall be referred to Arbitral Tribunal as prescribed by Ministry of Law, Government of India.
- The place of the arbitration shall be Gandhinagar, Gujarat.
- The Arbitration proceeding shall be governed by the Arbitration and Conciliation Act of 1996 as amended.
- The proceedings of arbitration shall be in English language.
- The arbitrator's award shall be substantiated in writing. The arbitration tribunal shall also decide on the costs of the arbitration procedure.
- The expenses of the arbitration as determined by the arbitrators shall be shared equally between the two parties. However, the expenses incurred by each party in connection with the preparation, presentation shall be borne by the party itself.
- Arbitration clause shall be only applicable in case of dispute is arising out of contract. The said clause shall not be applicable in the case of cyber-crimes and any other type of confidentiality/security breach relating to PHI carried out by either bidder organization itself or its employees.

5.24 Books & Records

The selected agency shall maintain adequate documents related to project's materials & equipment's etc for inspection and audit by the TENDERER during the terms of Contract until expiry of the performance guarantee.

5.25 Performance Guarantee

- The Selected agency shall furnish Performance Guarantee as provided in the bid document to the TENDERER for an amount 5% of the total contract value.
- The performance guarantee will be in the form of bank guarantee for the amount equal to amount mentioned above towards faithful performance of the contract obligation, and performance of the equipment during Warranty period. In case of termination of contract, the TENDERER shall invoke the PBG.
- The Performance Guarantee shall be valid for a period of 180 days beyond Contract period and shall be denominated in Indian Rupees and shall be in the form of an unconditional Bank Guarantee issued by all Public-Sector Banks/private banks

having branch in Gandhinagar/Ahmedabad in the format provided by the TENDERER to be submitted Within 21 calendar days from the date of final work order.

- The Performance Guarantee shall be discharged by the TENDERER and returned to the successful bidder within 30 calendar days from the date of expiry of the Performance Bank Guarantee on demand or request of SI.

5.26 Termination by the TENDERER:

The TENDERER, reserves the right to suspend any of the services and/or terminate this agreement in the following circumstances by giving 30 days' notice in writing if: -

- The bidder becomes the subject of bankruptcy, insolvency, and winding up, receivership proceedings; In case the TENDERER finds illegal use of hardware, software tools, manpower etc. that are dedicated to the project.
- If SLAs are not maintained properly and not provide services as per SLAs, then TENDERER has right to foreclose contract.
- Upon occurrence of an event of default as set out in Clause above, either party will deliver a default notice in writing to the other party which shall specify the event of default and give the other party an opportunity to correct the default.
- Upon expiry of notice period unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the Agreement.
- During the notice period, both parties shall, save as otherwise provided therein, continue to perform their respective obligations under this Agreement and shall not, whether by act of omission or commission impede or otherwise interfere with party's endeavor to remedy the default which gave rise to the commencement of such notice period.
- The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.
- In case of termination bidder will be paid for the work/services already delivered till the date of termination after deduction of penalties, if any.

5.27 Indemnification

Selected agency will defend and/or settle any claims against the TENDERER that allege that Bidder service and/or branded product as supplied under this contract infringes the intellectual property rights of a third party. Selected agency will rely on Customer's prompt notification of the claim and cooperation with our defense. Bidder may modify the product or service so as to be non-infringing and materially equivalent or we may procure a license. If these options are not available, we will refund to Customer the amount paid for the affected product in the first year or the depreciated value thereafter or, for support services, the balance of any pre-paid amount or, for professional services, the amount paid. Bidder is not responsible for claims resulting from any unauthorized use of the products or services. This

section shall also apply to deliverables identified as such in the relevant Support Material except that Bidder is not responsible for claims resulting from deliverables content or design provided by Customer.

5.28 Limitation of Liability

Selected agency's cumulative liability for its obligations under the contract shall not exceed the value of the pending part of the assigned orders anytime by the TENDERER within the contract term on the day claim is raised.

5.29 Confidentiality

- Selected agency understands and agrees that all materials and information marked and identified by the TENDERER as 'Confidential' are valuable assets of the TENDERER and are to be considered as proprietary information and property. Selected agency will treat all confidential materials and information provided by the TENDERER with the highest degree of care necessary to ensure that unauthorized disclosure does not occur. Selected agency will not use or disclose any materials or information provided by tenderer without its prior written permission.
- Selected agency shall not be liable for disclosure or use of any materials or information provided by the TENDERER or developed by selected agency which is:
  - Possessed by selected agency prior to receipt from the TENDERER, other than through prior disclosure by the TENDERER, as documented by selected agency's written records.
  - Published or available to the public otherwise than through a breach of Confidentiality; or
  - Obtained by selected agency from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to the TENDERER; or
  - Developed independently by the selected agency.
- If selected agency is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, selected agency shall promptly notify the TENDERER and allow reasonable time to oppose such process before making disclosure.
- Selected agency understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause the TENDERER irreparable harm, may leave the TENDERER with no adequate remedy at law and the TENDERER is entitled to seek to injunctive relief.
- The TENDERER does not follow the practice of asking Confidential Information of selected agency, however if any confidential information is required/shared by the selected agency then selected agency must clearly have marked it as "Strictly confidential". The TENDERER in turn will not share the same without prior concern of

the selected agency.

- Above mentioned "confidentiality clause" shall be applicable on both the parties i.e. the TENDERER and the successful bidder.

5.30 Service Terms

- The entire scope of the work depends on the technical skill and experience in management of the same level or kind of capabilities.
- The Bidder must submit regular schedule of manpower availability.
- The Bidder will need to coordinate and approach various departments/Sub-departments/ Boards/Corporations during this contract.
- The Bidder is responsible to maintain documentation on the progress of the work and will have to update the same on regular basis. Bidder will have to submit the progress reports regularly, as per the guidelines issued by TENDERER from time-to-time.
- TENDERER shall provide office space to the operational consultants in its own premise during project period. All other expenses related to transportation, consumables, stationary, printing, scanning, telephone, food, snacks, etc. in case required, must be completely borne by the Bidder as part of Contract Agreement.
- The bidder shall ensure that security measures, policies and procedures implemented are adequate to protect and maintain the confidentiality of the Confidential Information. Bidder also agrees and acknowledges that it shall adhere to reasonable security practices over all sensitive personal information of the said project as prescribed by various rules under I.T. Act, 2000 (as amended from time to time).

5.31 Fraudulent and Corrupt Practices

- Fraudulent practice means a misrepresentation of facts to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the TENDERER of the benefits of free and open competition.
- "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official in the process of Contract execution.
- The TENDERER will reject a proposal for award and may forfeit the EMD and/or Performance Bank Guarantee if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing, contract(s).

5.32 Patent Rights, Copy Right & IPR

- The Service Partner shall indemnify tenderer against all third-party claims of infringement of copyright, patent, trademark or industrial design rights arising from use of the Goods/services. In the event of any claim asserted by a third party, the Bidder shall act expeditiously to extinguish such claim. If the Bidder fails to comply and tenderer is

required to pay compensation to a third party resulting from such infringement, the Bidder shall be responsible for the compensation to the Tenderer including all expenses, court costs and lawyer fees.

5.33 Approvals/ Clearances

- Necessary approvals/ clearances concerned authorities, for establishing the proposed project needs to be obtained by the selected agency.

5.34 Exit Management Procedure

- This Schedule sets out the provisions, which will apply on expiry or termination of the Contract Period and/ or earlier termination of the SP and/ or the SLA for any reasons whatsoever.
- In the case of termination of the Project implementation and/or SLA due to illegality, the parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
- The parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.
- The Exit Management Period starts, in case of expiry of Contract, 6 months before the Contract comes to an end or in case of earlier termination of Contract, on the date of service of termination orders to the Service Partner. The Exit Management Period ends on the date agreed upon by the tenderer or six months after the beginning of the Exit Management Period, whichever is earlier.
- During the Exit Management Period, the Service Partner shall use its best efforts to deliver the Services. Payments during the Exit Management Period shall be made in accordance with the Terms of Payment Schedule.
- The selected Service Partner will be required to provide necessary handholding and transition support to the tenderer's staff or its nominated agency or replacement Service Partner. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.
- The Service Partner shall permit the tenderer and/or any replacement Service Partner to have reasonable access to its employees and facilities as reasonably required by the tenderer to understand the methods of delivery of the Services employed by the Service Partner and to assist appropriate knowledge transfer.

5.35 Extension of Work

At the end of the contract duration, i.e., 7 years, performance of the selected bidder may be reviewed, and the contract may be extended up to 3 Years on mutual consent from both the parties or till the time of selection/onboarding of the new agency.

5.36 SUPPORT FROM EXTERNAL AGENCY

Sub-letting of the extension of the GFGNL connectivity services to connect urban government offices through sps with or without leveraging gfgnl infrastructure engagement is strictly not permitted. The bidder needs to complete all the defined activities as per scope of work under his supervision. However, No Data/ Information should be sent out of the premise without obtaining prior written confirmation from the TENDERER.

5.37 EXIT MANAGEMENT PROCEDURE

i. This Schedule sets out the provisions, which will apply on expiry or termination of the Contract Period and/ or earlier termination of the PIA and/ or the SLA for any reasons whatsoever. An Exit Management plan shall be furnished by PIA in writing to the Tenderer within 60 days on completion of the contract period or termination of the contract for default of the PIA, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation and Service Level monitoring.
ii. A detailed program of the transfer process that could be used in conjunction with a Replacement PIA including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
iii. Plans for provision of contingent support to Project and Replacement PIA for a reasonable period after transfer.
iv. Exit Management plan in case of normal termination of Contract period.
v. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
vi. Exit Management plan in case of termination of the PIA.
vii. In the case of termination of the Project implementation and/or SLA due to illegality, the parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
viii. The parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.
ix. The Exit Management Period starts, in case of expiry of Contract, 3 months before the Contract comes to an end or in case of earlier termination of Contract, on the date of service of termination orders to the Service Provider. The Exit Management Period ends on the date agreed upon by the tenderer or six months after the beginning of the Exit Management Period, whichever is earlier.
x. During this period, the Service Provider should:
    a. Deliver the services.
    b. Provide necessary support to the Tenderer's staff, nominated agency, or replacement Service Provider.
    c. Permit reasonable access to its employees and facilities to the tenderer and/or any replacement Service Provider for knowledge transfer.
xi. Payments during the Exit Management Period shall be made in accordance with the Terms of Payment Schedule.

xii. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.

xiii. The Service Provider shall permit the tenderer and/or any replacement Service Provider to have reasonable access to its employees and facilities as reasonably required by the tenderer to understand the methods of delivery of the Services employed by the Service Provider and to assist appropriate knowledge transfer.

xiv. Exit Management plan at the minimum adhere to the following:

1. Three (3) months of the support to Replacement PIA post termination of the Contract
2. Complete handover of the Planning documents, bill of materials, technical specifications of all equipment, user manuals, guides, IPR, network architecture, change requests if any reports, documents, and other relevant items to the Replacement PIA / Tenderer
3. Certificate of Acceptance from authorized representative of Replacement PIA issued to the PIA on successful completion of handover and knowledge transfer
4. In the event of termination or expiry of the contract, Project Implementation or Service Level monitoring, both PIA and Tenderer shall comply with the Exit Management Plan.
5. During the exit management period, the PIA shall use its best efforts to deliver the services.

5.38 USE OF AGREEMENT DOCUMENTS AND INFORMATION

- The Bidder shall not without prior written consent from TENDERER disclose the Agreement or any provision thereof or any specification, plans, drawings, pattern, samples or information furnished by or on behalf of TENDERER in connection therewith to any person other than the person employed by the Bidder in the performance of the Agreement. Disclosure to any such employee shall be made in confidence and shall extend only as far as may be necessary for such performance.
- The Bidder shall not without prior written consent of TENDERER make use of any document or information made available for the project except for purposes of performing the Agreement.
- All project related documents issued by TENDERER other than the Agreement itself shall remain the property of TENDERER and Originals and all copies shall be returned to TENDERER on completion of the Bidder's performance under the Agreement, if so, required by the TENDERER.

5.39 TAXES & DUTIES

Bidder is liable for all taxes and duties etc. as may be applicable from time to time.

- Quoted prices shall be on all- basis i.e., including all taxes, duties, local levies, transportation, loading-unloading charges, packing, forwarding, freight & insurance etc.
- Statutory variation in the rate of GST, taking place between the date of award of contract and the original / refixed delivery period or service period, shall be to the

Tenderer's account. For claiming any change in price due to such Statutory variation, the successful bidder shall have to lodge claim before the Tenderer providing documentary evidence of change in rate of GST taking place after the date of award of contract and the date of supply within the original / refixed delivery period. Tenderer shall issue necessary amendment in the contract to enable generation of supplementary invoice or revised invoice as the case may be.

- No increase in price on account of statutory increase in the rate of GST taking place during the period of delivery period extension with liquidated Damages shall be admissible. Nevertheless, the Tenderer shall be entitled to the benefit of any decrease in price on account of reduction in GST taking place during extended delivery period.
- If Credit Note pertaining to Penalty (Non Refundable) has been raised, then GST `need not be imposed. If Credit Note pertaining to other than penalty (Non Refundable) has been raised, then GST need to be imposed.

5.40 Risk Purchase:

I. If the selected Bidder (referred to as H1 here in this clause) fails to perform its obligations (or any part thereof) under this scope of this RFP or if the scope of this RFP is terminated by the Tenderer due to breach of any obligations of the selected Bidder under scope of this RFP, the Tenderer reserves the right to procure the same or equivalent Hardware / Services / Deliverables from other sources as per options mentioned below.
   a. from H2 / H3 /…Hn Bidder (where n is the total number of bids received with the first Bidder out of H2 / H3 /…Hn who agrees to match the price of H1 discovered rate of H1.
   b. from any other "alternate source". The procurement from "alternate source" shall be done, as far as possible, through Government's procurement guidelines as deemed appropriate by the tenderer.

II. Above mentioned procurement will be done at the selected Bidder's (who has failed to perform its obligations & thus defaulted) risk, cost and responsibility. Any incremental cost borne by the Tenderer in procuring such Hardware / Services / Deliverables shall be borne by the selected Bidder (who has failed to perform its obligations & thus defaulted). Any such incremental cost incurred in the procurement of such Hardware / Services / Deliverables from other source will be recovered from the pending due and payable Payments / Security Deposit / Bank Guarantee provided by the selected Bidder (defaulted Bidder) under this scope of this RFP and if the value of the Hardware / Services / Deliverables under risk purchase exceeds the amount of pending payable payments / Security Deposit and / or Bank Guarantee, the same may be recovered, if necessary, by due legal process.

III. In this case of risk purchase, H1 Bidder or H2 / H3 /…Hn Bidder or any alternate source will have to submit performance bank guarantee @ 5% of the total value of the work allotted to the Bidder.

5.41 Delivery Timeline

- Successful bidder has to complete the Installation, Configure, Commissioning, Integration with Acceptance of the ordered work within the time period (s) specified in the below table. However, in case of any delay solely on the part of successful bidder. TENDERER reserve the right to levy the appropriate penalties as per the below table:

Sr. No	Particulars of Payment	Completion Timeline (in Weeks) T = Date of Award of Nprocure Contract/LoI	Payment Terms
1	Submission of PBG	T + 3 Weeks	NIL
2	a. Project Kick-off b. Technical architecture – IT Infra c. Technical architecture – Network infra d. Configuration of functional requirement of software GIS and NMS on bidders cloud as per RFP Solution. Design Document with detailed HLD, LLD, Deployment Plan, Testing Plan, Risk Management Plan, Change management plan, O&M Plan, etc.	T + 3 Weeks	NIL
3	Demonstration of prototype/screen/functional work flow of GIS and NMS as per RFP	T+5 week	10% of the total Project Value
4	Delivery of Hardware for IT Infra and Network infra	T + 6 Weeks	20% of the total Project Value
5	Demonstration of finished software for GFGNL on Bidder's cloud	T + 10 week	10% of the total Project Value
7	a. Completion of Installation, Integration, testing of complete digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with Bharatnet S-NOC (C-S-NOC) at New Delhi & Bengaluru	T + 15 Weeks	20% of the total Project Value
	b. Successful completion of FAT, completion of training and Go-live	T + 17 Weeks	10% of the total Project Value

Sr. No	Particulars of Payment	Completion Timeline (in Weeks) T = Date of Award of Nprocure Contract/LoI	Payment Terms
8	Operation & Maintenance	7 Years from Go live	30% of the total Project Value as Equated quarterly payments, after the end of each quarter calculated from Go-Live
9	Manpower for O&M Phase	Day-0 from Go-live	Man month Payment based on calculation on discovered cost on Quarterly Basis
10	Supply, Installation, integration, Testing and FAT of field components as per scope at each location.	4 Weeks from the date of order issued to agency.	

Note:

- Material supplied, installed and commission as per this Bid/contract should be covered under the warranty for a period of five years from the date of FAT.
- CAMC (Comprehensive Annual Maintenance Contract) value for each year should not less than 7 % of CAPEX Value
- Aforesaid penalty cap will not be applicable for any severe impact/incident/outage at GSDC, resulting in loss to Government of Gujarat.
- In case of any fault arises in the installed items during the warranty period of five years, bidder is requiring to either repair the faulty items or have to install the
- replacement (complying to the RFP specification) for faulty material without any additional cost to the Tenderer.
- No advance payment will be made.
- All payments will be subject to penalties for delays, as specified in the Service Level Agreement (SLA). In case of any penalties applied due to delays or non-compliance with SLAs, the corresponding deductions will be made before processing payments.
- The financial offer submitted by the Bidder must be in conformity with the payment terms proposed in the tender.
- Each payment shall be made on receipt of separate invoice on the successful completion of payment schedule.
- The selected proposer's request for payment shall be made to the purchaser in writing, accompanied with the supporting documents describing, as appropriate, the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
- Documents required, whichever applicable along with documents for desired deliverables, to be

submitted to GFGNL for Payment (in Triplicate):

- Initial training completion certificate signed by nodal officer: This shall be a document mentioning the start and end date of the program, along with information about batch attendance, training material, etc.
- Due payments shall be made by the purchaser within thirty (30) days after submission of a valid invoice and all required supporting documents along with request for payment by the selected proposer, and the purchaser has accepted it.
- The currency or currencies in which payments shall be made to the selected proposer under this Contract shall be Indian Rupees (INR) only.
- All remittance charges will be borne by the selected proposer.
- In case of disputed items, the disputed amount shall be withheld and will be paid only after settlement of the dispute.
- Any penalties and/or liquidated damages, as applicable, for delay and non- performance, as mentioned in this bidding document, will be deducted from the payments for the respective deliverables.
- Taxes, as applicable, will be deducted/paid as per the prevalent rules and regulations.

Operational Penalty:

- The successful bidder shall repair/ replace all faulty material covered under the warranty within the shortest possible time thus ensuring minimum downtime at any site, failing which applicable penalty will be imposed. In case of failure of appliance / solution for more than 3 consecutive time for the same issue, bidder would be bound to replace the product with no cost to GOG.
- The successful bidder shall be responsible for maintaining the desired performance and availability of the system/services.
- Successful bidder should ensure the prompt service support during warranty period.
- Timeline for resolution is within 24 hours from date of call logged / reported to Bidder/OEM. If the successful bidder fails to resolve the call as specified above, penalty will be imposed on each delayed day for 3000 Rs / Day, which will be recovered against payable or from Performance bank guarantee submitted by the successful bidder on completion of warranty period.

FINAL ACCEPTANCE TEST: To be carried out based on followings but not limited to:

- Successful implementation, compliance of all technical and functional specifications and scope mentioned in the RFP
- After successful installation of the System in accordance with the requirements as mentioned in Schedule of Requirement, Final Acceptance Test will be conducted. After successful testing, Acceptance Test Certificate will be issued by DST/its designated agency to the successful bidder. FAT Checklist is as per Form below:
- The date on which Acceptance certificate is issued shall be deemed to be the date of successful commissioning of the System. Warranty and licenses should be valid for period of 7 years+3 years extendable from the date of issuance of Acceptance Certificate (FAT).
- Any delay by the successful bidder in the Acceptance Testing shall render the successful bidder liable to the imposition of appropriate Penalties.
- All goods and services that are not specifically asked for certification should have quality standard applicable in India such as ISI.

5.42 Payment Procedure

- The TENDERER shall certify actual implementation. Bidder has to ensure proper handholding & support of the system.
- SP shall raise the component wise invoice as per the milestones achieved as mentioned above in the payment schedule & submit the invoice to TENDERER.
- TENDERER shall verify the Invoice raised against the milestone achieved & shall make the payment after deduction of penalty, if any.
- The SP's request(s) for payment shall be made to TENDERER along with the 2 original copies of invoice and necessary documents. The invoice should be in English language and Gujarat based.
- Payment shall be made in Indian Rupees. While making payment, necessary income tax and other applicable taxes deductions will be made.

SECTION-6 SCOPE OF WORK

6.1 Scope of Work

(i) BharatNet State Network Operation Centre (S-NOC) shall be required to monitor the up time, qualitative parameters of the BharatNet network and provisioning of the services as mentioned in the RFP. The fundamental purpose of this RFP is to provide technology led governance of the entire network including automation in service provisioning, scanning of the network health, digital routes for identifying fiber location, digital measurement book, digital SLA and top level dashboard and techno savvy next generation SPV (GFGNL).

(ii) The S-NOC will cater the requirement of monitoring of implementation, O&M activities & utilization of BharatNet Network, which will have extended up to villages in Amended BharatNet program. Successful bidder shall serve the Supply, installation, commissioning, and maintenance of S-NOC infrastructure up to 10 years.

(iii) Bidder shall be responsible for design, validation, implementation and post implementation operation and maintenance of S-NOC for 10 years. Bidder shall also be responsible for complete IP scheme design and allocation as per requirement, third party integration, monitoring of all components, configuration of all devices, monitoring all devices through NMS/EMS, Helpdesk/Service desk solution, cabling works of supplied devices and connection with GFGNL devices at core including districts and Edge locations. Coordination with multiple agencies for project execution, Compute and storage solution, Network time protocol device for time synchronization with all devices, follow guidelines- GOI, TRAI, GOG, DST, supplied device with all required licenses, features as per requirement etc. Bidder is free to add the component/device/server/services to meet the operational requirement.

(iv) Bidder is also responsible to provide necessary guidance, documents, training and technical work-flow information to other agency for integration.

(v) Successful bidder shall be responsible to provide separate logins (NMS/EMS, OSS+BSS+CRM, Helpdesk etc.) for multiple agencies and shall be responsible for maintain audit trail.

(vi) Successful bidder is responsible to coordinate with GFGNL team for integration with GFGNL devices, traffic management from Central & Cluster/Zone/District to GP level through GFGNL media (DWDM, Router, OLT, ONT, Switch, CPE), resolve all the technical issues.

(vii) The BharatNet State Network Operation Centre(S-NOC) shall comprise of various Network components like Core Switch, Router, Server, firewall that manages Open & Multi-Vendor Access Points, OSS+BSS+CRM.

(viii) Bidder shall be responsible for integration of S-NOC with BBNL through API or any other possible way.

(ix) The S-NOC shall provide a unified platform to facilitate the effective utilization of BharatNet. It will support operational and commercial activities through key modules, including but not limited to:

a. Trouble Ticketing
b. Customer Relationship Management (CRM)
c. Fiber Management for monitoring fiber cuts and faults
d. Public Grievance Management
e. Reporting Functions

f. SLA Monitoring and Management for ILL, network, and connection services
g. Subsidy Management
h. Project Monitoring Tools
i. Asset Management and Monetization Tools
j. Performance Monitoring for field staff and fault teams

(x) S-NOC shall be manned with qualified manpower for S-NOC operations. S-NOC shall be managed 24x7x365 and accordingly manpower to be planned. S-NOC shall always be able to generate inventory report of active elements like port status, port utilization status etc. for future perspective through Network Management System (NMS). S-NOC would also maintain necessary reports like details of no. of nodes per logical links on any particular fibre route through NMS.

6.1.1 Real-Time Data Access

The S-NOC will provide real-time operational status of OLTs/ONTs (GPs), Wi-Fi access points, FTTH connections, and more. This information will be accessible via web and app interfaces and integrated with the Digital Bharat Nidhi (DBN) Project Monitoring tool.

6.1.2 AI-Driven Data Analytics and Security

The S-NOC will include a Data Lake for AI-based analytics and visualization, offering granular insights into network status, utilization trends (geographical, income-based, educational, etc.), and more. It will also ensure robust data and network security at all levels and provide features for performance optimization and risk visualization.

6.1.3 Reporting Capabilities

The S-NOC will generate comprehensive reports for DBN and stakeholders, including but not limited to:

- GP uptime/downtime, including weekly progress
- Fiber optic cable cuts and performance
- Node (OLT, router) status, with a 12-month time series
- Data consumption at GPs and nodes
- FTTH connection status and usage reports
- Live FTTH connection status dashboards

6.1.4 Granular Reporting

The S-NOC will generate state-wise, district-wise, block-wise, and GP-wise reports detailing:

- Media type, commissioning dates, and work status
- Implementation phases, Wi-Fi/access point activity
- FTTH connections (provided/active)
- Dark fiber leasing, bandwidth leasing, and data consumption

6.1.5 API Integration

The S-NOC shall enable API-based integration or any other proven way to integrate and share data with BSNL S-NOC, and S-NOC/ billing systems of ISPs to share network-related information seamlessly.

6.1.6 Infrastructure and Fault Records

The S-NOC shall maintain comprehensive records of the OFC transport network, including:

- Equipment details, fiber inventory, and connectivity
- Bandwidth allocations for service providers
- Traffic types at nodes
- Faults and rectification logs, service provider-wise

6.1.7 Central and State S-NOC Interconnectivity

State S-NOCs will be interconnected with the Central S-NOC via APIs. The health of state S-NOCs will be monitored centrally.

6.1.8 SLA-Based DCN Link Monitoring

The dimensioning and cost of DCN links connecting BharatNet EMS to S-NOCs (central/state) shall be considered. These links shall be SLA-based with penalties and monitored via the S-NOC.

6.1.9 Dashboards for Stakeholders

State/UT-specific dashboards shall provide quality, quantity, and other details for local administration. Centralized billing/monitoring dashboards shall also be made available to union ministries and departments funding BharatNet services. API integration with dashboards like those of NITI Aayog, PMO, and DoT will be facilitated.

6.1.10 Complaint and Grievance Management

The S-NOC shall include systems for managing complaints and grievances, including:

- Subscriber Complaints: Web portals and call centers for issues related to service quality, billing, etc.
- General Complaints: Systems for grievances from BNU, vendors, sub-vendors, and stakeholders, including queries and suggestions.

6.1.11 DC/DR Sites

- The proposed solution should be implemented in DC & DR sites. GFGNL will provide the space and power for DC site at Gandhinagar and DR site at Baroda or other city as per feasibility of GFGNL.
- Bidder has to arrange the DR site and connectivity with scalability and availability.
- Both the sites shall be in high availability mode.
- GFGNL will use the DR site setup compulsorily during DR Drills.
- Bidder shall plan DR as per the requirement of GFGNL for the critical applications or as per process.

6.1.12 DR Drill

The bidder has to conduct at least one DR Drill in each quarter, for the solution and as and when required by GFGNL without any additional cost to the GFGNL.

- Bidder shall provide necessary Hardware, Software and supporting licenses for remote access server for all the OEM for proposed solutions.

6.1.13 Bidder & OEM Responsibilities

(i) Plan, design, and configure the supplied equipment in alignment with the provided layouts.
(ii) OEM along with the bidder has to ensure design and technical compliance of the proposed solution and has to ensure all service support during entire contract period.
(iii) The overall strategy of implementation is divided in two parts.
(iv) The one part is, technical configuration, right traffic engineering/re-engineering, identification of stress point, and overall solution within one jurisdiction and one pocket (i.e.one block and one district, internet breakout, Intranet) and with an objective to validate and freeze the technically implementable aspects with active role of expert which is OEM in this case.
(v) The second part is, to replicate the above rightly defined model jointly concerned by OEM and GFGNL for further replicate with improvements if any by the bidder.
(vi) The failure during this pilot pocket shall be the good reason for termination of the entire work order without any scope of negotiation or doubts.
(vii) The bidder shall provide all the resources and handful intent to complete this round of work as per part of his quoted commitment.
(viii) OEM has to ensure successful implementation of pilot block and pilot district first which will be replicated in rest geography by bidder.

6.1.14 Existing Infra HOTO

- Bidder shall take the HOTO of existing IT infra like Video wall, computer terminals and Non IT infra like furniture, UPS. AMC of the these infra shall be responsibility of the bidder. Information is given in Annexure B.

6.1.15 Compliance w.r.t. DPDP Act. 2020

- Bidder shall be responsible for establishes a framework to meet the compliance of DPDP Act 2020 or latest.

6.1.16 Compliance w.r.t ISO 20000 and ISO 27001

- The bidder shall be required to deliver services in compliance to ISO 20000 and ISO 27001. In future, GFGNL is planning to get the S-NOC ISO 20000, ISO 27001 certified. In that case, bidder will provide all required documentation and support.

6.2 Design, Implement & integrate AI-Enabled Secure Core ICT Solution for BharatNet Gujarat

6.2.1 Establishing Secure ICT Infrastructure:

The RFP aims to establish a state-of-the-art, secure core ICT infrastructure, deploying automated tools to ensure smooth operations. This initiative is crucial for providing internet access to all villages and rural communities in Gujarat, enabling access to essential services like high-speed secure internet, education, healthcare, and e-governance services. This RFP marks an important step toward achieving digital inclusion in Gujarat under the BharatNet Project. GFGNL seeks a qualified bidder to manage the entire project lifecycle, from design and

planning to implementation, integration, and efficient operation and maintenance (O&M), by providing the related comprehensive solutions as per the line items mentioned in the RFP.

The bidder must deploy all ICT infrastructure as per the RFP at the State Data Centre, Gandhinagar, and may be required to deploy at any other location within Gandhinagar/Ahmedabad as specified by GFGNL in the future.

The selected bidder will be solely responsible for the design, supply, installation, testing, and commissioning (SITC), including O&M, as outlined in the RFP. This responsibility also extends to any future relocation within the Gandhinagar/Ahmedabad geographical boundary. Any associated shifting costs will be borne by the bidder, with no additional charges payable by the tenderer.

6.2.2 Enhancing Core Network Connectivity:

This Request for Proposal is focused on enhancing the core network infrastructure, with the bidder required to collaborate with the ABP PH-III Project Implementation Agencies (PIAs) across both packages. These both PIAs are responsible for infrastructure extending from the State Data Centers (SDC) down to the Gram Panchayat (GP) level through fibre and router to last mile. The overarching goal is to deliver a secure network and internet access to over 14,654 Gram Panchayats and extend the connectivity to all other government offices and FTTX customer located beyond these Panchayats.

6.2.3 Managing Internet Access & Security:

The primary Internet source will be the National Knowledge Network (NKN), with supplementary internet access provided through secondary Internet Service Providers (ISPs). The bidder is responsible for developing and implementing a solution that manages internet and intranet traffic from both ABP PH-III packages while ensuring compliance with the RFP's internet access requirements. The bidder must also provide a solution for user registration and authentication at the individual, department, or office level. This includes creating a user ID and password system to ensure secure internet access, fully compliant with regulatory, Indian ISP compliance. Additionally, the bidder will be responsible for managing the collection of necessary logs, such as internet access records, session management, IP, MAC details, and other relevant data, in compliance with ISP regulations and Indian laws, and for the required duration.

6.2.4 Automating Processes & Digital Milestones:

Additionally, this core network infrastructure and the associated software will support virtualized access technologies, inspections, and tools to validate and automate processes for verifying digital milestones, as outlined in the ABP PH-III. This includes defining processes and workflows, addressing stakeholder gaps, and offering automated systems for payment and validation. The bidder is encouraged to propose and outline the tools or technologies that can fully automate the processes and systems to meet all requirements without manual intervention.

6.2.5 Incident Resolution & RCA:

The bidder must propose a comprehensive solution as per the ABP PH-III, considering uptime and SLA management processes. This includes identifying, analyzing, and integrating alarms related to faults, performance, configuration, and service etc. After integration, the bidder must provide valid Root Cause Analysis (RCA) for each fault in the incident and trouble tickets. The

bidder is responsible for designing and validating all integration-related solutions to prepare an automated SLA system based on incident RCAs.

6.2.6 Automated SLA & Performance Reporting:

The bidder must ensure that no manual intervention is required to calculate the SLA module. The SLA system should provide detailed reports on equipment uptime, including RCA, for daily, weekly, monthly, quarterly, or any custom date ranges. The system should generate detailed reports categorized by issue type, technology led, zone, district, and block, GPs, IP/MAC etc. and not limited to this may require to develop as per future requirement raise by GFGNL. Bidder has to develop solution and require to prepare Meta data by (creating unique code/id/using LGD code etc.) of the scope of all gram panchayat locations, other all government offices locations of BharatNet project and based on this location- bidder has to design and implement monitoring dashboard and all the reports. If any element is deleted in EMS that should be reported as down in the monitoring tool/dashboard and respective incident or ticket also need to generate automated for such incident.

6.2.7 Core Network & Cloud Infrastructure Design:

The project involves designing and implementing a robust core network infrastructure that includes high-performance network devices like BNG, core WAN router, and core switches, Firewall etc. So, Redundancy and failover mechanisms will maximize network availability. The network design shall optimize routing protocols and traffic management that has to ensure by Bidder. The bidder will also design and implement an enhanced private cloud environment with advanced switching technologies and robust computing resources. This environment will host all the EMS of ABP PH-III OEM of both package. Physical infrastructure, including data center racks and cabling, SFPs, and not limited to this but all the require accessories will be designed and implemented by bidder at the SDC.

6.2.8 Traffic Management & Security:

BharatNet Phase 3 is divided into two package: Package A and Package B, further both package has been divided into three zone each. So, total Six zones are created and all the intranet traffic of all zones will be handed over to respective zone wise by respective package PIA to this Core infrastructure bidder of this RFP and has to ensure that all the traffic has been managed and forwarded to provide secure internet thoroughly all require process of authentication. Bidder has to ensure that there should not be any unauthorized traffic of any package/zone is able to access internet of any office, gram panchayat, user, h-connectivity, ftth etc. Bidder of this RFP has to provide DNS, DHCP, IPAM, Private, and Public IP planning in coordination with ABP PH-III both Package PIA and is solely responsible for implementing the same.

6.2.9 OSS-BSS & NMS Integration for Service Management:

The bidder is required to deploy and plan an integrated OSS-BSS (Operational Support System - Business Support System) and NMS (Network Management System), ensuring that all customer orders—covering all types of customers and services—are properly managed and integrated with the proposed OSS-BSS system. This integration must support the full lifecycle of services, from provisioning to monitoring, management, and eventual termination. The OSS-BSS solution should enable the effective handling of all service-related activities, ensuring seamless coordination across all service stages. Additionally, the bidder is encouraged to propose any cost-effective solutions that could enhance the functionality or value of the system,

beyond the core requirements specified in this RFP. Furthermore, all proposed core infrastructure components, software modules, and related solutions must strictly comply with the latest technical specifications defined by the TEC GR (Telecommunication Engineering Center - Generic Requirements) for the respective line items, modules, or electronic components, ensuring alignment with industry standards and regulatory guidelines.

6.2.10 ICT Security, Policy, VAPT & Risk Mitigation:

Security is paramount. The bidder will be responsible for planning of IT security policy and require to create security posture for all the ICT infrastructure of GFGNL. Not limited to that bidder has to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VA-PT) for the GFGNL Cloud and all network components of GFGNL network components which will includes the Amendment BharatNet program and other consecutive Phases. All software requirement to perform VAPT will be the scope of bidder and additionally, the bidder must facilitate a third-party security audit as and when performed by GFGNL or authorized agency and hardening for critical devices to ensure the security of the infrastructure. Bidder has to resolve all the vulnerability within stipulated time and need to consider CVSS 3.0 and the latest scoring for severity need adhere in operation and maintenance phase (i.e. 7 + 3 years). Severity category and resolution time has been provided in the VAPT penalty section 7.11 of this RFP and need to resolve all the potential vulnerabilities. Security team has to ensure all the necessary postures are updated in the GFGNL environment.

6.2.11 Security & Compliance Framework:

The bidder will be responsible for ensuring compliance with various essential policies that contribute to the security and resilience of the infrastructure. These include but not limited to:

I. Organization Security Policy: Define the overall approach to information security across the organization.

II. Access Control Policy: Regulate access to systems, data, and networks to ensure that only authorized personnel can access sensitive resources.

III. Data Protection and Privacy Policy: Safeguard personal and sensitive data, ensuring it is handled according to legal and regulatory requirements.

IV. Network Security Policy: Protect the network infrastructure from internal and external threats, ensuring the integrity and availability of network resources.

V. Incident Response Policy: Effectively manage and respond to security incidents in a timely manner to minimize damage and recovery time.

VI. Acceptable Use Policy (AUP): Define the acceptable use of organizational resources to prevent misuse and ensure compliance with security standards.

VII. Vendor and Third-Party Management Policy: Ensure third-party vendors comply with security standards and align with organizational policies.

VIII. Business Continuity and Disaster Recovery Policy: Ensure continuity of operations during disruptions and establish recovery procedures to minimize downtime and data loss.

IX. Logging and Monitoring Policy: Define the types of events to log and ensure comprehensive logging and monitoring to detect potential security threats.

X. Employee Training and Awareness Policy: Educate employees on security best practices to mitigate human error and ensure a security-conscious workforce.

XI. Physical Security Policy: Protect physical assets and facilities from unauthorized access, ensuring the integrity of physical security controls.

XII. Change Management Policy: Manage changes to core IT systems and infrastructure to ensure that modifications do not introduce vulnerabilities or disruptions to services.

The bidder will ensure all these policies are created and need to implement as when require by the GFGNL, should be maintained, and monitored to safeguard the organization's digital and physical assets while ensuring business continuity and compliance with industry standards.

6.2.12 Multi-Layered Security & Network Protection:

The bidder will design and implement multi-layered security, including a next-generation firewall with intrusion prevention and diction system. The bidder will deploy and integrate key software solutions securely for network management, operations, business functions, and user access, including systems like DNS, Syslog, GIS, NMS, OSS, BSS, SDN, AAA, network visibility, project monitoring, and helpdesk module etc.

6.2.13 ABP PH-III Integration & NOC Coordination:

For ABP PH-III integration, the bidder will establish communication with PIAs and OEMs, track progress, create FCAPS templates, and define SOPs. GFGNL holds the ISP license. The bidder will procure and manage MPLS LLs for UNMS NOC integration and coordinate with stakeholders. The bidder will integrate with UNMS Delhi and Bangalore NOCs, providing data via APIs. The bidder is responsible for procuring and managing MPLS LLs for Bangalore and Delhi UNMS NOC integration, including backup lines, and coordinating with stakeholders. Regarding UNMS integration and monitoring, the bidder will establish connectivity and integrate with the UNMS Delhi and Bangalore NOCs, providing GIS, inventory, FCAPS, and service provisioning details via APIs.

6.2.14 ISP Compliance, Regulatory, TRAI & other Legal Support:

On behalf of GFGNL, the bidder must ensure full compliance with all ISP regulatory requirements, including TRAI guidelines and other legal mandates. All internet access must be authenticated, with necessary logging of user activities as per ISP regulations. The bidder is responsible for planning, procuring, and managing the Public IP Pool and MPLS Leased Lines (LL) in coordination with GFGNL, which holds the ISP license. The solution must strictly adhere to Indian regulatory and security standards, ensuring lawful internet usage, data retention policies, and compliance with any future regulatory updates.

6.2.15 Migration & Expansion of Core Infrastructure:

Bidder has to create and migrate over core infrastructure for facilitate internet for all the gram panchayats, horizontal offices, GISL Wi-Fi services, and other P2P services which are already running in the Phase 2. Tentative count of all the services of Phase 2 are 25000+ and phase 1 will be the scope of Bidder.

6.2.16 Governance Model & Digital SLA Development:

The RFP provides a technical detail to design and build over all technology led governance model. The GFGNL has issued BharatNet Phase 3 RFP and backhaul RFP. The potential participants are advising to go through BharatNet Phase 3 RFP and backhaul RFP, milestones for further mapping in preparing live NOC, digital SLA, digital payments, work flows and various network elements for the integration purpose. The selected vendor will develop a detailed project plan. Line items are minimum and indicative expectations, and bidders are encouraged

to offer enhanced functional specifications for better outcome propose modifications.

6.2.17 Training & SOP Development:

Bidder shall provide all the kind of training and module wise SOP to all the employees of GFGNL, all the team members of respective stakeholders during the project and once in every year of O&M phase.

6.2.18 Third-Party Audits & Quality Assurance:

Regarding FAT, Audits, and Quality Checks, GFGNL may nominate Third Party agencies for FAT, milestone payments, invoice validation, audits, or quality checks, and the bidder must provide necessary documents. Concerning Support, GFGNL will provide administrative support.

6.2.19 RFP Modifications & Compliance Obligations:

GFGNL reserves the right to modify or remove any components at any stage of the RFP process in pursuit of cost-effective solutions. Bidders must comply with these changes.

6.3 4S vision

GFGNL's endeavor to connect all the villages across the State of Gujarat to foster growth and bridging the digital divide. Service delivery is the key priority for GFGNL, SI shall be responsible for overall objectivity and operational functionality to support technology led network governance and automation.

4S – Services
Service Portfolio,
Service provisioning,
Service Performance Monitoring,
Service Audit and Security Compliance

defined as following in deployed network but not limited to,

a) **Service portfolio:** Following Services should be supported in proposed solution.
   - Grass root level E-governance,
   - E-GRAM
   - Digital enterprise,
   - Internet peering service,
   - Wireless broadband,
   - Govt Network (SWAN),
   - Enterprise VPN,
   - Community Wi-Fi,
   - Education content push from central,
   - Bank and ATM connectivity related services,
   - Videoconferencing for Tele-medicines and government administrative activities,
   - Digital transformations,
   - CCTV camera services,
   - Open Network for Data Commerce (ONDC), e-Commerce and Internet of Things (IoT)

Sr. No	Service Type	Service Outcomes	Network Expectations
1	**Telemedicine @ Primary Health center in Gram panchayat**	• Enable seamless high-quality video calling & multi-party video consulting • Transfer for Dicom (Digital Imaging and communication in Medicine) images for X ray, MRI	a) Unicast, Multicast and Broadcast services b) Point to Point, Point to Multi Point and Multi point to Multi point service c) Secure connectivity – MPLS service for any to any connectivity d) Low latency on this service is mandatory e) Real time service KPI monitoring and handling traffic accordingly f) Service resiliency
2	**Enabling govt. schools with online education**	• Enabling high quality content delivery from servers across the state • Enabling interactive video education • Teacher to teacher training and attendance marking	a) Unicast, Multicast and Broadcast services b) Point to Point, Point to Multi Point and Multi point to Multi point service c) High bandwidth for HD quality content d) Low Jitter, delay free service e) Monitor real time KPI of service and take action to ensure quality of service f) Service resiliency
3	**Anganwadi office connectivity**	• Data transfer from village to applications in Centralized location	a) High speed connectivity
4	**Govt. Offices**	• Data transfer – Digital Sewa Setu • Video conferencing • Cloud application access • Internet access	a) Unicast, Multicast and Broadcast services b) Point to Point, Point to Multi Point and Multi point to Multi point service c) Secure connectivity – MPLS service for any to any connectivity d) Low latency on this service is mandatory e) Real time service KPI monitoring and handling traffic accordingly f) Service resiliency

Sr. No	Service Type	Service Outcomes	Network Expectations
			g) Service monitoring from Govt. office to service endpoint in real time with reporting h) Data transfer including jumbo frames
5	**Home broadband connectivity**	• Consistent internet delivery – Movie • internet access at high speed • ISP content delivery	a) Enable multiple LCO's & MSOs to connect to GFGNL b) Internet traffic segmentation of different providers over GFGNL network c) Secure internet peering with different operators at block locations d) Internet route handling capacity across all active infrastructure for all operators e) Internet peering capability
6	**Telco service**	• Connecting remote telco towers • Enabling segmentation for different telco operators from tower location	a) Enable multiple telco 's to interconnect b) Support telco synchronization requirements c) Interconnect & segment different telco traffic d) 99.99% uptime for telco connectivity services e) Service protection for telco to be automated

b) Service provisioning (Automated):

Proposed Solution shall comply Zero-touch provisioning for all type of services. Proposed solution should support the end-to-end services from State capital to Last remote level entities as and when required to the following segments, but not limited to,

- Government Segments (Panchayats, Schools, Agriculture, Animal husbandry, Community health, Anganwadi, Police, Food and civil supplies)
- Power Segments (Electricity distribution, utilities, and solar companies)

- Financial market (Cooperative banks, Private banks, non-banking finance companies and Insurance, Stock exchange intermediaries)
- Agriculture Segment (Fertilizer shops, Seeds and pesticides retail chains, Agriculture mandis, APMC, Commodity traders)
- Education Segments (Digital aided learning centers, Private schools, Libraries, Hostels and even at rural citizen homes with “Har Ghar Education” campaign through FTTH partnership model)
- Business enterprises (Logistics and transport, Retail chain, Hotel chain, Digitization anywhere, Remote factories)
- TSP/ISP Segments and Households

As the network is being rolled out, ability of the network to monitor and run varied services on deployed network with service SLA’s and quality of experience is one of the base objectives. Continuous and real time service provisioning and monitoring has become of paramount importance. The selected bidder needs to ensure that the proposed solution should seamlessly interwork with the details as given below.

All the above defined services need to be provisioned in the network in an automated manner from the S-NOC (Network Operations Center). The key network functionalities which will enable these services to be delivered as per the requirements defined are mentioned below:

1. Proposed Solution should have the capability to provision L2 and L3 services against all the proposed active elements based on.
2. Enabling the Service definition to be defined with network functionalities, the solution proposed should have ability to visualize Segment Routing/MPLS-TE policies and VPN services as an overlay on the network topology map.
3. Proposed Solution must be able to provision and visualize EVPN and ELAN services.
4. Proposed Solution must support service specific constraints, such as bandwidth, latency, path diversity, and traffic engineering constraints, such as affinity, bandwidth, cost, latency coming from the network.
5. Proposed Solution must be able to provision QoS, Multicast and their VPN services.
6. Proposed Solution must visualize RSVP-TE and VPN services as an overlay on logical network and geographical maps.

c) Service Performance Monitoring (Qualitative Service Visibility):

Proposed solution shall populate the Network performance monitoring dashboard containing the network KPIs such as

- Service UP/DOWN,
- No. of Fiber cuts,
- MTTR,
- Lossy Fiber,
- Repetitive fiber cuts,
- Ageing for Service restoration,

- Quality of fiber splicing,
- Classified performance measures,
- Real-time historical statistics and trouble-shooting events,
- Throughput and Utilization,
- Latency, Jitter and Packet Loss

at administrative hierarchy to maintain like Village, Gram Panchayat, Block, District and State capital level on Daily-Monthly-Quarterly-Yearly basis for network troubleshooting as per SLA commitment as well as for Service performance visualization to various Government leadership team which should build transparency between the Government and Citizens on digital services.

Below are the key functional requirements to enable continuous network and service performance measurement across the GFGNL network.

1. The Proposed solution should have an architecture supporting ease of deployment, zero touch maintenance and seamless monitoring could be on premise or MeitY empaneled cloud based.

2. The Proposed solution should support following multiservice monitoring like Education service, Anganwadi service, tele health service, government applications and the following ISP, SaaS based applications, BGP prefix/routing, DNS, Multi Cloud, SD-WAN, Hybrid WAN, Network device health, VPN gateway, and VoIP.

3. The proposed solution should support synthetic network test at both ends of a monitored path (GP to S-NOC or GP to Internet), enabling testing of the path in either or both of two directions: source to target or target to source. It should provide standard network metrics: packet loss, latency, jitter, and optionally throughput–an improved form of the bandwidth metric–along with Path Visualization and path MTU.

4. The proposed solution must support two options for the L3 service path tracing ICMP and TCP. Solution must support network path visualization: a time-correlated, unified view of all paths between any two points on your network. With visibility across network, application, routing, and device layers. Solution should support three(min) and ten(max) parallel path traces from each agent/vantage points on network to try and discover multiple paths leading towards the target.

5. The Proposed solution must support multiple integration with 3rd party Analytic platforms like ITSM platforms like ticketing tools using Webhook, API and Open telemetry.

6. The proposed solution should be able to monitor the individual ISP Links for all hosted applications. Solution should have the ability to automatically detect Internet outages in ISP networks to help identify the problem area of outages.

7. The proposed solution should support monitoring of Internet-based connectivity and Service from user / office to GFGNL S-NOC or SDC connectivity, the more thorough and capable path monitoring means faster trouble domain isolation, faster triage, and better escalation processes.

8. The proposed solution should monitor the cloud-based unified communication and collaboration platforms like MS teams, Webex, Zoom, Google meet etc. of any other defined for their performance monitoring.
9. Real time visibility & monitoring of both Network and Application(s) for better co-relation of the Service impact pro-actively rather than re-actively. (Milli Second Level visibility: 20pps to 1000 pps for real time monitoring) for continuous real time KPIs and SLA reporting.
10. The proposed solution should be able to clearly visualize the Hop-by-Hop visibility of the Underlay Network at a granular level Sub-Second) for Identifying clear problematic sections on the Glass pane view.
11. The proposed solution should be able to perform Predictive Analytics for Better Network Planning.
12. The proposed solution should be able to perform Service Activation testing in an Automated way and provide easy downloadable reports for link handovers.
13. The proposed solution should have the Observability glass-pane which could ingest and demonstrate both network and Application SLA's on a Single glass-pane as per the requirement.
14. The service originating from end devices like routers at government offices or ONT at residence, the performance and quality measurement in terms of peak speed, total data consumption, server reachability should be monitored continuously in real-time and a dashboard for the same has to be created.
15. Latency measurement of each service from end device at customer premise should be done in real time and actions should be taken to rectify is issues seen.

d) Service Audit and Security compliance:

1. PIA should match the industry standard and government specific security compliances for all type of services to be provisioned in deployed network and should support all the service audit requirements.
2. Authentication of all the active devices in the network should be managed by a central authenticator, it should support role-based access, authentication, authorization and accountability capabilities.
3. All the changes made in any active network element has to be logged with timestamp and log in details for future audits.
4. All the software's used by the active network elements has to be validated by a software integrity check program and the ability of the active network elements to do the same has to be demonstrated by the bidder and his OEM.

5. Active network element should ensure that while the device boots there is a validation of the software being used by the device.
6. Network segmentation in terms of management network, operation network and out of band network for management access only has to be maintained in the network.
7. S-NOC security – Implement security measures as per industry best practices and CERT-in guidelines to fortify the S-NOC infrastructure against potential cyber threats or any other security lapses.
8. MD-5 (Message Digest Algorithm) route authentication for all static and dynamic routing protocols.
9. The S-NOC security solution shall be capable of discovering and prioritizing events occurring across the network. It shall also determine the risk level by identifying the assets that are affected and recommend and/or execute the appropriate remediation response mechanism.
10. Enable prevention and containment of threat based on abnormal activity through early notification/alerting of suspicious activity and also have the ability to quickly respond to a containment mechanism.
11. The Protocol and security compliance related to the supplied product has to be ensure by the Bidder and OEM as specified DoT/TRAI/GoG/CERT/etc. Thus, offered product /solution must adhere to security norms, prevailing security practices and it should not limit functionality of security activations.

6.4 Geographical Information System (GIS):

1. Gujarat Fibre Grid Network Limited (GFGNL) intends to procure services of a competent firms for establishing a GIS system to help in management, analysis, and display of its fibre network to be created (accurately to 20 cm geographical precision) as part of BharatNet Phase III implementation with seven (7) years of operations & Management.
2. Intended use of envisioned GIS is for Optical Backhaul and Access Network layout planning, capturing of field data, tracking OFC route, auto computing project progress by displaying Video/Photos to virtual inspection team, viewing MIS reports from NMS and viewing web dashboard.
3. As per the requirements of Amendment Bharatnet to suffice the requirements of virtual inspection and digitally driven project functionality of Deliver, Draw and Discover to be adopted with the help of GIS, detailed specification mentioned in Annexure A part 2.
4. GIS software and manpower provided to operate the same shall be compatible with the GIS mapping procedure mentioned in annexure A Part 1
5. Survey team will provide the information/data and feed the same into GIS. Implementation team will provide the information as the work get completed on everyday basis.
6. Above two points will complete the Deliver marker. Secondly as built is to be completed which makes the confirmation work for data submitted by the team.

7. Lastly equipment which shall be integrated into S-NOC by completion of commissioning, gets discovered in GIS also. So, third marker will get completed and payment milestones of project completion to be mapped which trigger the payment procedure on keeping delay penalty into account.
8. Submeter accuracy(20cm) to be achieved with DGPS.
9. GIS to be integrated with NMS so on single window/umbrella multiple information can be visible.
10. Videography and visualization on web portal is to be done as per the ask in BharatNet phase III RFP and also mentioned in technical specification.
11. API integration with different applications like RFMS, OSS, BSS and ERP is to be done as per technical specification.
12. User management as per the role to be done describe in technical specification.
13. The solution must bundle GIS layers for block boundaries, GP, and village locations. Additional necessary layers for network planning should also be provided- describe in technical specification.
14. Administrators should be able to attach forms or checklists, setting mandatory fields as part of the workflow or network process- describe in technical specification.
15. GIS software shall support desktop planning with fibre network design topology, including ring-based and linear-based structures with shortest route determination. Also able to place infra elements like pole, manholes, duct. Further requirements are described in fibre inventory management and network modelling of technical specification.
16. GIS software shall be able to use template-based modelling for configurable design specifications.
17. GIS software shall be able to calculate the power and loss as per the user configurable and fetching real time NMS/EMS data.
18. GIS Software shall be able to provide feasibility of dark fibre, fibre distance between any two points as per the ask of administrator and also be able to integrate with ERP for penalty calculation of Dark fibre.
19. GIS Software shall be able to provide real time monitoring of passive and active equipment and also be able to assist in cut scenario, network equipment failure scenario.
20. GIS Software and its mobile app shall be able to provide on line and offline functionality of data capturing to creating entities and notifications.
21. GIS to be provided reports as per the need by bidder/PIA/TPA/IE.
22. During project phase, Bidder shall provide 4 numbers of GIS operators who are responsible for planning, authenticating and MIS work for reports generated from GIS.
23. GIS Software shall be able to provide FRT and patrolling management which includes life cycle management of TT and WO. Also be able to suggest the movement and optimal work assignment to team and leave management, attendance management. Further requirements are described in Field operation management.
24. GIS Software and its mobile app shall be able to provide measurement book functionality as per ask in amendment BharatNet project for validation of work, project timelines, task dependencies and milestones. Further Penalty calculation based on the as built data which comprise of soil strata mentioned in BSNL ABD RFP, trench depth asked in GFGNL ABD RFP achieved trench depth and non-use of trench depth protection between markers are to be

calculated, reports to be generated in excel and PDF as per custom requirement.

25. Identification of route through GIS OFC link ID with chainage marking are also to be done.
26. GIS Software and its mobile app supplier shall provide training all concerned stack holder who are using the functionality directly or indirectly.
27. Bidder shall customize the supplied tool as per additional requirements by GFGNL.
28. Any Software upgrade change request shall be free of cost. GFGNL will not pay extra amount for upgrade or change request to deliver any functionality asked by GFGNL during contract period.
29. The bidder is required to develop the application and all associated forms in accordance with Videography Section (5.8) of the BharatNet 3 program amendment and its subsequent phases. The scope of the bidder includes ensuring that all video applications forms/function with length and timestamp as intended for various objective. Additionally, the bidder must support all necessary requirements for creating a digitized video/photo geotagging tool, forms in web and mobile as and when required or executed by GFGNL and bidder has to support to define SOP with PIA of Phase 3.

6.5 Operational Visibility Platform (NMS + OSS + BSS):

The proposed solution should work as a software layer/platform for the management of entire Bharat Net project in the state of Gujarat for the GFGNL. The proposed OVP solution should have complete functionality of Network Management System (NMS), Operations Support System (OSS), Business Support System (BSS) etc. or we can say it will be the combination of all these IT tools/system to fulfill the requirement mentioned in this section. The system shall serve a large-scale network. It must operate across multiple vendors while integrating with SNMP, SSH, and IP-based reachability for client and device management.

The Network Management System (NMS) shall be required to provide a scalable, automated, and vendor-neutral solution for network deployment, monitoring, and service management across multi-vendor IP and optical infrastructures. The system will streamline operations, ensure SLA compliance, and support end-to-end lifecycle automation with mobile-based deployment, GIS-based topology visualization, and OEM-engineer backed customization.

MIS Report:
solution should be able to generate the following reports but not limited to

Sr. No	Report Type / Category	Specifications	Periodicity
1	Dashboard Reports	Shows N/W availability, Average BW available vs Usage per GP, Latency, Jitter. Custom dashboards for Managing Director, Senior Management & Field Offices in a readable format.	Daily
2	Bandwidth Availability & Utilization	Available bandwidth per of Router, ONT, OLT, Mini OLT and switch devices Taluka/Block-wise, District-wise, and	Daily

Sr. No	Report Type / Category	Specifications	Periodicity
		State-wise. Bandwidth Utilization (Max, Min, Avg) per GP Ring, Block Ring, and District Ring.	
3	Device Availability & Performance	Availability of Router, ONT, OLT, Mini OLT and switch devices (Live vs Faulty) PoP-wise, Block-wise, District-wise, and State-wise. CPU, Memory, and BW utilization of Routers & Switches.	Daily
4	Fault & Incident Management	Total No. of Complaints Raised. Trouble Ticketing & Life Cycle Management for Network & Service Problems. Ageing Report of Issues/Complaints/Incidents.	Daily & Monthly
5	Network Performance & Monitoring	Network KPIs (Up/Down Status), SLA Monitoring, Real-time Traffic Monitoring, Threshold Alerts, and Zoom-in Analysis down to the port and IP level. Historical reports for various periods.	Daily & Weekly
6	Receive Signal Strength Monitoring	ONT/Router/Mini OLT signal strength tracking with alert triggers when below the defined threshold.	Daily
7	Configuration Management	Auto discovery of devices, Resource Inventory Management, Service Template Management, and Configuration Change Reports.	Quarterly
8	Preventive & Scheduled Maintenance	Preventive maintenance reports, Scheduled maintenance tracking, and Software upgrade/enhancement reports.	Quarterly & Monthly
9	Security & Access Management	Role-Based Access Control (RBAC), Operator Authentication, Audit Logs, Helpdesk Module with SMS/Email Notification.	As Required
10	Network Topology & Mapping	End-to-end network topology connectivity till the last mile CPE, dynamic discovery of fibre connectivity.	As Required
11	Inventory & Asset Management	Inventory Reports including Dark Fibre Availability, Number of Fibre Used, and Penalty Calculation. End-to-end Asset Lifecycle Tracking including hardware, software, and license management.	Quarterly
12	Reporting & Data Extraction	Reports with drill-down features (package-wise, district-wise, block-wise, ONT/Router/Mini OLT and switch -wise). Tabular and Graphical reports with extraction in Excel, CSV and PDF format.	D/W/M/ Q/Y

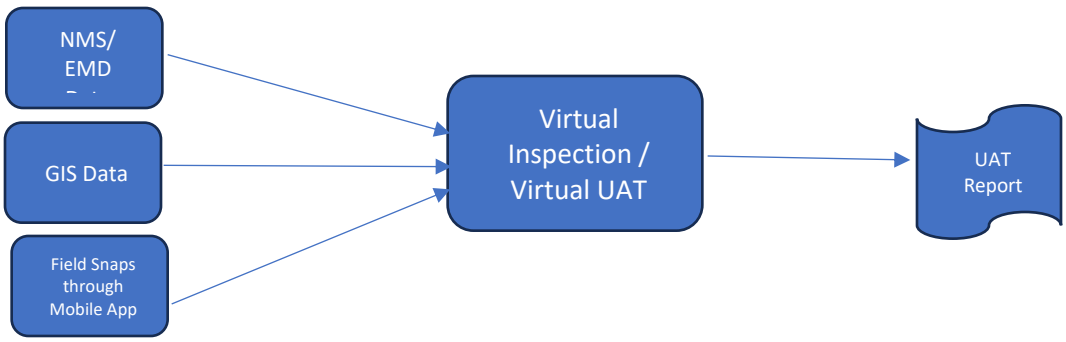
Sr. No	Report Type / Category	Specifications	Periodicity
13	SLA Compliance & Billing	SLA monitoring, SLA computation, and SLA-based billing generation for partners and end clients. Penalty % of O&M amount tracking.	Quarterly
14	Service Performance & Uptime Analysis	Service Availability, Downtime, Usage/Utilization, Fault & Rectification, Performance Statistics, and % Uptime Achieved.	As Required
15	Compatibility & Integration	NMS should support SNMP, JAVA, CORBA, XML, REST API, and integration with OEM APIs. The system must support both legacy and future technologies for seamless data exchange.	As Required
16	Any Other Reports	Within the reporting framework with flexibility of rapid customization.	As Required

The Bidder shall be responsible for developing a Platform for conducting virtual Inspection and user acceptance testing. The Application shall be hosted in S-NOC

The developed platform shall be integrated with NMS/ EMS, GIS and

The Application shall be capable enough to conduct a virtual inspection of field from any geography. This inspection will happen with live video environment.

The required infra shall be in the scope of bidder.



6.6 Manpower requirement on Payroll of SI (No Subcontracting is allowed):

Any deviation to this will be considered free manpower.

Sr. No	Designation	Qty	Education Qualification, Relevant Experience & Technical Certification	Roles & Responsibilities
1	**Data Centre Project Manager**	1	a) B.E. CE/IT or any relevant engineering discipline & MBA/Post Graduate/Prince 2/PMP Certified b) Minimum 6+ Years of Post Qualification experience in managing Data Centre/ICT operations c) CCIE/CISSP/CCNP/CISA/CISM/ CDCP or ITIL/ISO 27000 or relevant data center-specific certifications in Cloud/VMware	Overall in charge, responsible for GFGNL Core ICT infrastructure that includes Network, Security, Software, and Cloud environment. Define work flow, manage the core team
2	**Cloud Specialist**	1	a) B.E. CE/IT or any relevant engineering discipline b) Minimum 5+ Years of Post Qualification experience in Management of Private Cloud Resources, vCPU, RAM, Storage, Exp. In managing 40-100 VMs a) OEM Certified for Cloud platforms (Any AWS/ Azure/Google etc.)	Manage cloud infrastructure, design cloud architectures, implement best practices, and oversee the deployment and management of cloud-based services and resources.
3	**Security Expert (Security Compliance Officer)**	1	b) B.E. CE/IT or any relevant engineering discipline c) Minimum 5+ Years of Post Qualification experience in Network Security Management d) CISSP/ CISM/ CEH/ CISA/ CompTIA Security+/ CompTIA CySA+/ CCSP/ ITIL/ISO 27001	Implementation of Security Policy, perform vulnerability assessments, handle incident management, and implement security protocols for networks and cloud systems. Ensure the security of data, applications, and networks. Manages compliance, and acts as a Compliance officer.
4	**Security Engineer**	1	a) B.E. CE/IT or any relevant engineering discipline	Responsible for network security, including configuration, monitoring, and response to security

Sr. No	Designation	Qty	Education Qualification, Relevant Experience & Technical Certification	Roles & Responsibilities
			b) Minimum 3+ Years of Post Qualification experience in Network Security management c) CCSE / PCNSE / CEH / SSCP / GCIH / GCFA /CompTIA Security+, CompTIA CySA+	incidents. Implement security measures to protect data, software, and hardware.
5	**Network Specialist (L3)**	1	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in Network Management c) CCIE / CCNP / JNCIP or related	Manage network architecture and infrastructure. Handle troubleshooting, performance optimization, and implementation of advanced network solutions.
6	**Network Engineer**	1	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 2+ Years of Post Qualification experience in Network Management c) CCNA or equivalent	Provide technical support for the network infrastructure, including installation, configuration, troubleshooting, and maintenance of network equipment and services.
7	**Systems Admin**	1	a) B.E. CE/IT or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in software development/ system engineer/integration c) Relevant software development certifications	Develop, manage, and maintain software applications within the data center. Ensure proper integration of applications with hardware and network systems.
8	**Database Admin**	1	a) B.E. CE/IT or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in database management, store, backup, securing, and optimizing databases c) Relevant database certifications (e.g., Oracle/ Microsoft SQL etc.)	Manage, secure, and optimize databases. Ensure the performance, availability, and integrity of data. Handle backup, storage, and daily operations of database applications. Implement Data Retention Policy

Sr. No	Designation	Qty	Education Qualification, Relevant Experience & Technical Certification	Roles & Responsibilities
9	**NMS Operations Engineer (API & Developmen t Expert)**	2	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in NMS Product specialist/ API/ development, configuration, monitoring, and management etc. c) OEM Manpower	Integrate, Configure, monitor, and manage Network Management Systems to ensure network performance and reliability. Troubleshoot and optimize the NMS to maintain network integrity.
10	**GIS Solutions Engineer**	2	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in GIS design, implementation, and maintenance c) OEM Manpower	Design, implement, and maintain GIS systems to analyze spatial and geographical data. Support network planning and management using GIS tools and techniques.
11	**OSS Integration Engineer**	1	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification in OSS systems integration and management c) OEM Manpower	Integrate and configure OSS systems to manage network operations, service delivery, and customer experience. Handle OSS-related issues and ensure seamless operation across platforms.
12	**BSS Solutions Engineer**	1	a) B.E. CE/IT/EC or any relevant engineering discipline b) Minimum 3+ Years of Post Qualification experience in integrating and managing BSS systems c) OEM Manpower	Integrate and manage business support systems (BSS) to handle tasks such as billing, CRM, and order management. Ensure the alignment of BSS systems with other business processes in telecom or IT operations.

- Bidder has to ensure availability of the manpower 24*7 in the NOC to provide network, software, security and related support to GFGNL, BharatNet Phase 3 PIA. This is minimum indicative list of resources and based on actual requirements bidder may deploy any number of resources to meet the SLA. GFGNL shall not pay any cost for additional resources deployed for compliance of SLA and completion of scope of work in due time.
- In case deployed staff is not available or is on leave, the bidder is required to provide the alternative personnel with same or higher technical capabilities of the non-available

personnel. Further, appropriate operational penalty will be levied in case of non-availability of minimum required manpower.

6.7 **Compute and Storage:**

1. GFGNL require Network Management System (NMS) and GIS which act as integrator for various element management system (EMS) for active elements involved in the project execution. In order to cater the requirements for hosting of above-mentioned applications and similar other relevant applications like AAA server, SMP, OSS, BSS, GFGNL intends to procure required System and Networking Hardware to be installed at State Data Center (SDC), Gandhinagar. These Applications shall have mix of Solaris, RHEL, Linux, Unix, CentOS and Windows platforms. The proposed hardware must support all these platforms for successful installation, commissioning & successful operation of applications. The prospective bidders should have proper experience and competence in the field to successfully complete the Scope of Work as mentioned in this RFP.
2. The scope is to supply, install and maintain the storage and compute solution at state data centre for GFGNL (including all active and passive components and sub-components) and necessary licenses, if any along with the 7 years of Comprehensive warranty and OEM Support at GSDC.
3. The bidder should provision the required hardware and software components which include Server Virtualization Layer, Servers, Physical Server management Module, Storage, etc. with appropriate licenses perpetual for life.
4. The Bidder has to ensure that if any additional component(s) required for overall solution to comply with the SLA levels, then in such case it should be the responsibility of the bidder to provide the same as a part of the entire solution.
5. Bidder shall incorporate the future requirements of sizing as per the description given in technical specification of storage.
6. The licenses should be in the name of GFGNL, Government of Gujarat valid perpetual for life.
7. The OEM support credentials should in name of GFGNL and handed over to GSDC/GFGNL.
8. The bidder is responsible for physical connectivity (within site) of the proposed solution. The required ports on switch for such connectivity will be provided.
9. The Bidder shall configure the proposed solution in such a way that it should comply with all the policies of the Gujarat State Data Centre.
10. The bidder along with the OEM professional should be available onsite for solution design, Installation, and implementation.
11. The bidder shall provide various documents like HLD, LLD and other technical documents of delivered product. The Bidder shall also share the Standard Operating Procedures Templates, Troubleshooting guide, “How-To” knowledge base, Escalation matrix etc.
12. The installation, implementation, commissioning, and migration shall be carried out by the OEM.
13. The bidder is required to submit the certification from the OEM of the proposed solution confirming successful implementation, testing, commissioning, and satisfactory deployment of the proposed solution based on the industry best practices as a part of FAT.Successful bidder in coordination with the representatives from the

GFGNL shall conduct FAT of the solution.

14. The Successful bidder shall be responsible for rectification of discrepancies identified by the TPA/any other authorized representative while conducting FAT. Further on rectification of all the discrepancies identified during the FAT, GFGNL representative will re-conduct the FAT or if agreed FAT will be signed.
15. The successful bidder shall be responsible for obtaining FAT certificate (Sign-off) on completion of the work as per the scope of work, functional and technical requirements.
16. The Bidder will be responsible for providing required training to the GSDC staff for further O&M.
17. The bidder should be authorized by its OEM and third-party OEMs to quote this bid for the authenticity, authorized representation and after sales support. The maximum response time to attend any onsite call should not exceed 4 hours from the initial call to the bidder / response center. The bidder is required to arrange back-to-back support agreement/arrangement for services including supply of spare parts with 24 hours' repair/replacement time commitment.
18. The bidder is required to provide back to back OEM support (24 x 7 x 365 days) for the period of 7 years from the date of successful completion of FAT. The entire deployed solution should be covered under the back to back OEM warranty till successful completion of FAT.
19. Bidder shall be responsible for operation and maintenance of the supplied components for the period of 7 years commencing from the date of successful completion of FAT.
20. Creating required no. of VM's for Hosting of various application on supplied infrastructure as per the direction of GFGNL.
21. Ensuring required configuration for maintaining virtual IP and switch where the VM's would communicate.
22. Bidder has to ensure that the application to be deployed does not disrupt the operations and affect other GSDC & GFGNL infrastructure in terms of performance and security.
23. Bidder shall provide Configuration of server parameters, operating systems administration and tuning.
24. Bidder shall provide operating system administration, including but not limited to resource contention, preventive maintenance and management of updates & patches to ensure that the system is up to date.
25. Bidder shall Re-install in the event of system crash/failures.
26. Bidder shall Maintain log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
27. Bidder shall perform event log analysis generated in all the sub systems including but not limited to servers, operating systems, applications, etc.
28. Bidder shall ensure that the logs are backed up and truncated at regular intervals.
29. Bidder shall do periodic health check of the systems, troubleshooting problems, analysing and implementing rectification measures.
30. Bidder shall upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract.
31. Bidder shall be Preparing, Implementation and maintenance of standard operating procedures for maintenance of the infrastructure based on the State's policies.
32. MIS Report:

Sr. No	Types of Reports	Periodicity
1	• Log of backup and restoration undertaken	Daily
2	• Summary of systems rebooted • Summary of issues / complaints logged with the OEMs. • Summary of changes done including major changes like configuration changes, patch updates (physical and virtual machines), etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.	Weekly
3	• Summary of component wise uptime. • Log of preventive / scheduled maintenance undertaken • Details of Patch, updates, Vulnerability fixes released and implementation status of same • Details of break-fix maintenance undertaken	Monthly
4	• Consolidated component-wise availability and resource utilization. • Reports as directed by the State for SLA calculation	Quarterly

6.8 Warranty Support:

As part of the warranty services bidder shall provide:

1. Bidder shall provide a comprehensive on-site OEM warranty of 7 years and 3 years extended warranty from (SI/OEM) from the date of FAT for proposed solution.
2. Extended warranty can be provided by SI on his own risk and cost basis.
3. Bidder shall also obtain the seven-years OEM premium support (ATS/AMC) on all licensed software, hardware, and other equipment for providing OEM support during the warranty period.
4. Bidder shall provide the comprehensive manufacturer's warranty and support.

   in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the bid. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this bid against any manufacturing defects during the warranty period.
5. Bidder shall provide the performance warranty in respect of performance of the
6. installed hardware and software to meet the performance requirements and service levels in the bid.
7. Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the bid.
8. During the warranty period bidder shall replace or augment or procure higher level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
9. If the solution fully /partially fails during FAT, the bidder must repair or replace by equivalent or higher-level of new equipment at no cost to the tenderer after approval from GFGNL/GSDC.
10. Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware

failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level of new equipment by the bidder at no cost.

11. For any delay in arrangement of replacement / repaired equipment's for inspection, delivery of equipment's or for commissioning of the systems or for acceptance tests / checks at each/ any site; GFGNL reserves the right to

    charge a penalty.
12. During the warranty period, the bidder shall maintain the systems and repair / replace the components to keep the solution operational at the installed site at no extra charges to the organization.
13. The bidder shall as far as possible repair/ replace the equipment at site.
14. Warranty should not become void, if DST/GIL buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.
15. Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
16. Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
17. Bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
18. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
19. Bidder shall develop and maintain an inventory database to include the registered hardware warranties.
20. To provide warranty support effectively, OEM should have spare depo in India and will be asked to deliver spare as per SLA requirement.
21. Management should be in HA, and required hardware, software, license and other components should be provided by bidder from the day-01.
22. Design, implementation should be done by OEM.
23. MIS reports should be submitted by bidders as and when asked by GFGNL.

SECTION-7 Service Level Agreement (SLA)

7.1 Penalties and Service Level Agreement (SLA)

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service, which shall be provided by the SP to tenderer for the duration of the contract for providing Applications, Operation and Maintenance support against the stated scope of work. Tenderer shall regularly review the performance of the services being provided by the SP and the effectiveness of this SLA.

7.2 Definitions

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings as set forth below:

a. "Incident" refers to any event / abnormalities in the functioning of TENDERER specified services that may lead to disruption in normal operations of TENDERER services.

b. "Response Time" shall mean the time taken after the incident has been reported at the concerned reporting center in resolving (diagnosing, troubleshooting and fixing) or escalating to (the second level, getting the confirmatory details about the same and conveying the same to the end user), the services related troubles during the first level escalation.

c. The "Resolution Time" shall mean the time taken for resolution of the problem and this includes provisioning of the work around to immediately recover the situation. The resolution time shall vary based on the severity of the incident reported.

d. "Availability" means the time for which the services and facilities are available for conducting operations of email service. Availability is defined as: {(Scheduled Operation Time – Service Downtime)/ (Scheduled Operation Time)} * 100%

e. Definitions of Severity Level:

Severity	Definition
1	Showstoppers involving major failure in the system/solution. There are no usable workarounds available to troubleshoot the problem.
2	Users face severe functional restrictions in the system/solution irrespective of the cause. Workarounds are time consuming.
3	Moderate functional restrictions in the system/solution irrespective of the cause. Has a convenient and readily available workaround. Affects a few users.
4	Requiring cosmetic functional changes. Does not require any workaround. It may include user query/suggestions but has no business impact

7.3 Interpretation & General Instructions

a) At the beginning of the contract, the SLA parameters and metrics thereof would be established by Purchaser in consultation with the selected bidder which would be reviewed

on an annual basis along with the Corrective Action & Preventive Action (CAPA) plan.

b) SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. In case the service levels cannot be achieved at service levels defined in the tables below, it shall result in a breach of contract and shall invoke penalties.

c) Penalties are mentioned as a percentage of certain components of cost.

d) Purchaser can take appropriate action including termination of the contract if –

   (i) Penalties calculations exceed 10% of the quarterly payment for two consecutive quarter.

e) The Bidder along with the product OEM's should support and prepare Root cause analysis (RCA) for all cases of Cyber Security Incidents and shared with Purchaser within 72 hours. Time extension can be granted by the Purchaser depending on the severity of the incident on request of the bidder. For any exceptions or SLA breach beyond the control of the bidder, the bidder may submit the RCA along with a justification, which may be considered by Purchaser. In case the RCA establishes that the breach on SLA was on account of email service issues, the bidder would be liable for the applicable penalty.

f) Root cause analysis (RCA) should be prepared for all cases of Severity 1 incidents causing email service unavailability or disruption. The bidder can work with OEM to provide the RCA.

g) For certain incidents, RCA may be carried out by Purchaser (or Purchaser appointed agency).

The Proposed solution should have its own comprehensive monitoring features. The bidder should use the same tool to do an integrated monitoring of the service levels for the deployed solution.

The bidder needs to carry out real-time monitoring as well as reporting of SLA parameters and will also be required to provide an integrated and automated monitoring report to Purchaser on monthly basis, or as requested by Purchaser. All SLAs to the extent possible should be monitored through the automated tools provided by the bidder.

7.4 Categories of SLA's

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The SP shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the SP shall be reviewed by TENDERER against this SLA. The SP shall:

- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract.

7.5 Project time lines, Payment milestones and Penalty During Implementation phase

Sr. No	Particulars of Payment	Completion Timeline (T*)	Related Penalties
1	Submission of PBG	T + 2 Weeks	EMD may be forfeited, and contract may be terminated or part thereof.
2	a) Project Kick-off b) Technical architecture – IT Infra c) Technical architecture – Network infra d) Configuration of functional requirement of software GIS and NMS on bidder's cloud as per RFP Solution. Design Document with detailed HLD, LLD, Deployment Plan, Testing Plan, Risk Management Plan, Change management plan, O&M Plan, etc.	T + 3 Weeks	From third week Onwards, A penalty of 0.02% of CAPEX value for delay for each Week or part thereof.
3	Demonstration of prototype/screen/ functional work flow of GIS and NMS as per RFP	T+5 Weeks	From third week Onwards, A penalty of 0.02% of CAPEX value for delay for each Week or part thereof.
4	Delivery of Hardware for IT Infra and Network infra	T + 6 Weeks	A penalty of 0.05% of CAPEX value for delay for each Week or part thereof. Delay beyond 4 Weeks, the TENDERER may also terminate the Work Order/Contract and forfeit the PBG.
5	Demonstration of finished software for GFGNL on Bidder's cloud	T + 10 Weeks	A penalty of 0.05% of CAPEX value for delay for each Week or part thereof. Delay beyond 4 Weeks, the TENDERER may also terminate the Work Order/Contract and forfeit the PBG.
6	a) Completion of Installation, Integration, testing of complete	T + 15 Weeks	A penalty of 0.06% of CAPEX value for delay for each Week or

Sr. No	Particulars of Payment	Completion Timeline (T*)	Related Penalties
	digital Platform including cloud, network and scope of physical infra and all software as per Project requirement. Integration with BharatNet S-NOC (C-S-NOC) at New Delhi & Bengaluru		part thereof. Delay beyond 4 Weeks, the TENDERER may also terminate the Work Order/Contract and forfeit the PBG.
	b) Successful completion of FAT, completion of training and Go-live	T + 17 Weeks	A penalty of 0.02% of CAPEX value for delay for each Week or part thereof.
8	Stabilization of the deployed Solution, Security certification and Go-Live.	T + 18 Weeks	A penalty of 0.05% of CAPEX value for delay for each week or part thereof. Delay beyond 4 Weeks, the TENDERER may also terminate the Work Order/Contract and forfeit the PBG.

*Note: **T = Date of Award of GEM Contract/LoI.**

7.6 Service Levels and Performance Penalty During O&M

The selected agency has to design the solution in such a way that the system uptime and service availability should be min 99.9%. The system uptime shall be measured per equipment on quarterly basis.

- Priority #1: System outage/ performance related issue effecting the overall functionality of the application.
- Priority #2: Having bearing on the day to day functioning of the deployed system/ availability of application (part functionality) for the GFGNL users, for example:

  Unable to provide /fetch the necessary parameters/details to other software system of GFGNL.
- Priority #3: Not having bearing on the day-to-day functioning of the deployed system.

Sr. No	Service Category	Breach Threshold	Penalty Amount
1	Service Availability	System availability falling below 99.9% in a calendar quarter	0.01% of contract value per hour of system unavailability exceeding the Threshold. The agency has to provide system generated monitoring report.

Sr. No	Service Category	Breach Threshold	Penalty Amount
2	Incident Resolution	Every Incident shall be logged with the priority Level and should be resolved in defined timeline. • Priority Level 1 Incident – Within 1 hour • Priority Level 2 Incident – Within 4 hours • Priority Level 3 Incident – Within 24 hours	Level 1 Incident 0.01% of Quarterly payment for every 1 hour or part thereof delay in resolution. Level 2 Incident 0.01% of Quarterly payment for every 4 hours or part thereof delay in resolution. Level 3 Incident 0.01% of Quarterly payment for every 24 hours or part thereof delay in resolution.
3	Security and Data Protection	a) Exceeding 24 hours for resolution time to security incidents	0.02% of contract value for each security vulnerability not remediated within timeframe specified by CERT-In which is immediate for Critical level, 24 hours for High level, 7 days for medium level and 15 days for Low level of severity
		b) Re-occurrence of vulnerability for which fixes were applied.	5% of contract value for each security vulnerability discovered
4	Data Backup and Recovery	Failure to perform scheduled backups or inability to recover data	5% of contract value for each missed backup
5	Support and Escalation	Exceeding 24 hours for fulfilment of support request or resolution of issues	INR 5,000/- per ticket per hour exceeding 24 hours

7.7 SLAs for Patch management / System Upgrades

All patches for released, to be tested for vulnerabilities, compatibility and any issues that may occur on deployment as defined in Patch Management Process. The patch cycle shall begin from the time of release of patches, testing, approval by purchaser as per change management and patch management processes and deployment on 100% of the target systems (Applications, Operating Systems, End-user devices, Network and Security components and tools, etc.). The bidder shall submit a report on the completion of patch activity.

SLA shall be calculated on actual delay time for the complete patch cycles on a quarterly basis for each patch from the date of release of patch by OEM. Detailed process should be discussed with the stakeholders and defined in the Operations Manual.
Patches shall be deployed on 100% of the system based on priority of the patches as per timelines defined below.

Sr. No	Priority	Timelines for complete Patch Cycle
1	Critical	1 day
2	High	3 days
3	Medium	30 days
4	Low	90 days

Sr. No	Target	Service Level	Impact Level/Penalty
1.	Patches shall be deployed on 100% of the system based on priority of the patches as per timelines defined	=100%	Nil
		>= 99% & < 100%	0.2% of the total Quarterly billing amount
		>= 98% & < 99%	0.5% of the total Quarterly billing amount
		>= 97% & < 98%	1% of the total Quarterly billing amount
		< 97%	2% of the total Quarterly billing amount

The bidder shall be responsible to upgrade the system/firmware of all applicable systems such as compute, storage, network components, security components, monitoring tools, and any other applicable device or tool used for providing forest management solution on a half-yearly basis. SLA shall be measured on delay of firmware upgrade in each applicable system component on a half-yearly basis.

Sr. No	Target	Service Level	Impact Level/Penalty
1.	100% systems upgraded within the half-year as applicable	=100%	Nil
		>= 99% & < 100%	0.2% of the total Quarterly billing amount
		>= 98% & < 99%	0.5% of the total Quarterly billing amount
		>= 97% & < 98%	1% of the total Quarterly billing amount
		<97%	2% of the total Quarterly billing amount

7.8 SLAs for Change Management

Sr. No.	Definition & Target	Service Level	Impact Level
1.	Changes as per the change request	100% of successful change implementation as per agreed timelines for each change request	Nil
		Delay in implementation of changes against agreed timelines for each change request	2% of the total Quarterly billing amount for each week of delay
2.	Unauthorized and un- approved changes done to the system without prior intimation and approval from Purchaser. Changes will be tracked through Configuration Changes and Compliance Monitoring Tool Target: No unauthorized or unapproved or unplanned change	Per unauthorized/ un- approved/un-planned change	5% of the total Quarterly billing amount

Note: Change management plan and timeline shall be mutually agreed between the purchaser and the selected agency.

7.9 Manpower related SLA and Penalties

1. Availability of the min required manpower should be 100%. The agency has to implement the attendance system and share the attendance report of each person deployed as part of team on monthly basis with the user department.

2. The agency is not allowed to replace those resources whose profile has been submitted at the time of Technical Presentation. Further in the event where the bidder is not able to retain the resources quoted in the bid, then the replacement must be pre-approved. For replacement, a panel consisting of 3 times the number of positions shall be submitted. GFGNL has a right to reject entire panel and seek substitute panel in the same 3 times proportion. Before replacing a resource, minimum two months' time to GFGNL along with panel has to be given to choose the substitution from the panel else penalties and pro-rata deduction in the quarterly fees will be made. We encourage the successful bidder to have a preapproved backup of resources for substitution for each of the positions.

3. Replacement of a profile by the agency (only one replacement per technical profile – with equal or higher qualification and experience – would be permitted per year)

4. Prior Intimated Leave of absence will be allowed: If a resource proceeding on leave or becoming absent is replaced with a resource approved by authority, then such substitution will not be treated as absence.

For every SLA non-compliance reported and proved, there shall be a penalty as given below:

Sr. No	SLA	Timelines/ Event	Applicable Penalty
1	Replacement of resources by the agency on formal submission of resignation by the resource in the company.	There should be minimum 15 days overlap between the new deployed resource and the replaced resource.	No penalty- On timely replacement. Rs. 5000/- per resource per day for each day delay from stated timelines.
2	The deployed resources shall not be engaged in any activity other than that assigned by the TENDERER	-	Penalty of Rs. 50,000 per resource may be imposed on breach of SLA. On consecutive breach of 03 times may lead to termination of the contract.
3	Absence without prior approval from the GFGNL.	-	As mentioned in table 3 per resource per day shall be imposed.

Table 3: Manpower Absent Penalty per Day

Designation	Penalty per day per resource
Data Centre Project Manager	5000
Security Expert (Security Compliance Officer)	4000
Security Engineer	2000
Network Specialist (L3)	2000
Network Engineer	2000
Cloud Specialist	2000
Software Engineer / Systems Engineer	2000
Database Admin	1500
NMS Operations Engineer (API & Development Expert)	1500
GIS Solutions Engineer	1500

Designation	Penalty per day per resource
OSS Integration Engineer	1500
BSS Solutions Engineer	1500

Note:

1 **Part thereof meaning:** if there is a delay of 9 days in the delivery then the penalty will be calculated as a (9/7) *Penalty Amount.

2 Calculation of Penalty will be done on periodic basis as defined in this document.

3 The penalty cap limit for CAPEX will be maximum to 20% of overall amount discovered in financial table for overall capex amount. And same will be applicable to 20% of overall amount discovered in financial table for overall OPEX amount.

4 The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 20% of Total Quarterly Payable. The penalties, if any, will be recovered against the quarterly payment invoice submitted by the agency. If the penalty exceeds for the two consecutive Quarter, then notwithstanding anything contained herein, the Purchaser may take appropriate action including the termination of the contract and forfeiting of the Performance Guarantee.

5 The agency shall be responsible to deploy appropriate tool to monitor the performance and submit system generated reports on the performance and adherence to the SLA. The user department shall also be able to pull the reports for verification.

6 The Tenderer holds the right to bring/deploy any external resources/agencies at any time for SLA review.

7.10 Software Penalty

Category	Description	Resolution Time	Penalty
Category 1: Bug Fixes & Security Breaches			
Level 1	**Critical Bug Fixes or Security Breaches**: Any software bug or security vulnerability reported to entire individual software application/server/ DB.	Within 8 hours from the time of reporting	• Rs. 50,000/- per incident • Rs. 1,000/- additional penalty will be applied beyond the mentioned resolution time until

Category	Description	Resolution Time	Penalty
Category 1: Bug Fixes & Security Breaches			
			issue get resolved on delay in applying the patch or fix.
Level 2	**Critical Security Breach**: Any system or application or module -related security breach affecting the overall functionality.	Within 24 hours from the time of identification	• Rs. 15,000/- per incident • Rs. 1,000/- additional penalty will be applied beyond the mentioned resolution time until issue get resolved
Level 3	**Software Crash or Data corrupted /Loss: Any incident that causes such incident that results into Data loss**	On time of reporting	• Minimum Rs. 25,000/- per incident • Rs. 1,000/- additional penalty will be applied beyond the mentioned resolution time until issue get resolved
Category 2: System Outage, API Related Issues, and Non-Functionality of Module			
Priority #1	System outage/performance issue affecting overall functionality, Software/Application Crash, DB corruption, Data loss etc..	Within 2 hours from the time of reporting	Rs. 5000/- per hour for each hour exceeding the resolution time.
Priority #2	Impacting day-to-day functioning e.g., inability to fetch parameters, data exchange failure with other systems modules	Within 4 hours from the time of reporting	Rs. 4000/- per hour for each hour exceeding the resolution time.
Priority #3	Issues related to API with the system, slowness in any FCAPS module, report generation, or improper functioning of integration that require improvement etc. or other detected during O&M	Within 24 hours from the time of reporting	Rs. 2000/- per hour for each hour exceeding the resolution time.
Category 3: Non-Availability or Incorrect Report			

Category	Description	Resolution Time	Penalty
Category 1: Bug Fixes & Security Breaches			
Type 1	**Non-Availability of Report/Data**: If any customized report fails to generate or is missing critical data (e.g., missing parameters or incomplete data).	On time of reporting	Rs. 500/- per incident
Type 2	**Incorrect Report/Data**: If any report is found to be incorrect (data mismatch, inaccurate calculations, etc.).	On time of reporting	Rs. 500/- per incident

7.11 VAPT Penalty:

VAPT Penalty Table based on severity levels and corresponding penalty amount:

Severity Level	Description	Resolution Timeframe	Penalty per Instance
Critical	High-risk vulnerabilities that can lead to a security breach, unauthorized access, or data leakage.	Must be resolved within 24 hours	• Rs. 2,000/- per hour or part thereof penalty will be applied beyond the mentioned resolution time until issue get resolved
High	Significant security gaps that can impact system integrity, availability, or confidentiality.	Must be resolved within 7 calendar days	• Rs. 1,500/- per hour or part thereof penalty will be applied beyond the mentioned resolution time until issue get resolved
Medium	Moderate security vulnerabilities that may not pose immediate risks but require timely mitigation.	Must be resolved within calendar 15 days	• Rs. 1,000/- per hour or part thereof penalty will be applied beyond the mentioned resolution time until issue get resolved
Low	Minor vulnerabilities that have a minimal impact but need to be addressed for compliance.	Must be resolved within 20 calendar days	• Rs. 500/- per hour or part thereof penalty will be applied beyond the mentioned resolution time until issue get resolved
Non-Compliance	Failure to conduct VAPT as per schedule or non-submission of compliance reports.	Immediate rectification required	₹10,000 per instance

7.12 Terms & Procedures of Payment

The GFGNL shall pay the successful agency in the following manner and at the following times, on the basis of the Price Breakdown given in this section on terms of Payment. Payments will be made in Indian currencies unless otherwise agreed between the Parties.

Payment during project stage:

1 Payment terms during project stage will be on project per milestone achieved in the implementation as mentioned in RFP document.

2 Payment during O&M services (post operationalization) will be equated quarterly payments calculated based on quoted service charges under O&M.

3 Payment during all stages of the contract will be subject to deduction of penalties for short comings in performance observed by GFGNL / User Departments / Third Party Audit agency.

SECTION-8 FINANCIAL BID

FINANCIAL BID FORMAT

Note:

1. L1 will be the lowest sum total of rates of all line items excluding GST.
2. GFGNL may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.
3. CAMC (Comprehensive Annual Maintenance Contract) value for each year should be 7 % of CAPEX Value

PART-A (Hardware & Software cost)

Sr. No	Particular	Qty	Unit Rate	Total Rate	Tax (%) as applicable
Supply Installation Testing and Commissioning with 7 years of warranty and support, update and upgrade					
1	GIS Application (For entire BharatNet Ph-1, 2,3 fiber route)	1			
2	Operational Visibility Platform (OVP) + OSS and BSS functionality	1			
3	DDoS - Distributed Denial-of-Service	1+1			
4	Next Generation Firewall	1+1			
5	Network Intrusion Prevention System (NIPS)	1+1			
6	Link Load Balancer	1+1			
7	BNG	1+1			
8	CGNAT	1+1			
9	Core Routers	1+1			
10	Core Switches	1+1			
11	Access Switches	1+1			
12	AAA Server	1+1			
13	Virtualization software	1			
14	Server	6			
15	Backup Server	2			
16	Backup Software for server	1			
17	Enterprise Storage	1+1			
18	Backup software for storage	1			

Sr. No	Particular	Qty	Unit Rate	Total Rate	Tax (%) as applicable
19	Endpoint protection	1+1			
20	Network Time Protocol Server	1+1			
21	DHCP-DNS-IPAM	1+1			
22	Syslog server	1			
23	Miscellaneous (cable. connectors, Racks etc.) in lot				
24	Any other components inadvertently missed out but require for overall solution and for compliance of RFP and GOG/GOI guidelines				
Total					

PART-B (Hardware & Software cost) for extended period of 3 years:

Sr. No	Particular	Qty	Unit Rate	Total Rate	Tax (%) as applicable
Extended 3 years of warranty and support, update and upgrade					
1	GIS Application (For entire BharatNet Ph-1, 2,3 fiber route)	1			
2	Operational Visibility Platform (OVP) + OSS and BSS functionality	1			
3	DDoS - Distributed Denial-of-Service	1+1			
4	Next Generation Firewall with	1+1			
5	Network Intrusion Prevention System (NIPS)	1+1			
6	Link Load Balancer	1			
7	BNG	1			
8	CGNAT	1+1			
9	Core Router	1+1			
10	Core Switches	1+1			
11	Access Switches	1+1			
12	AAA Server	1+1			
13	Virtualization software	1			

Sr. No	Particular	Qty	Unit Rate	Total Rate	Tax (%) as applicable
14	Server	6			
15	Backup Server	2			
16	Backup Software for server	1			
17	Enterprise Storage	1+1			
18	Backup software for Storage	1			
19	Endpoint protection	1+1			
20	Network Time Protocol Server	1+1			
21	DHCP-DNS-IPAM	1+1			
22	Miscellaneous (cable. connectors, Racks etc.) in lot	X			
23	Syslog server	1			
24	Any other components inadvertently missed out but require for overall solution and for compliance of RFP and GOG/GOI guidelines				
Total					

PART-C (Manpower Cost)

Sr. No	Resource Profile	Nos.	Duration (in months)	Unit Cost	Total Cost
1	Data Centre Project Manager	1	120		
2	Security Expert (Security Compliance Officer)	1	120		
3	Security Engineer	1	120		
4	Network Specialist (L3)	1	120		
5	Network Engineer	1	120		
6	Cloud Specialist	1	120		
7	Software Engineer / Systems Engineer	1	120		
8	Database Admin	1	120		
9	NMS Operations Engineer (API & Development Expert)	2	120		

Sr. No	Resource Profile	Nos.	Duration (in months)	Unit Cost	Total Cost
10	GIS Solutions Engineer	2	120		
11	OSS Integration Engineer	1	120		
12	BSS Solutions Engineer	1	120		

Note:

Total financial

Sr. No.	Description	Cost (Exclusive of Tax)
1	Part-A	
2	Part-B	
3	Part-C	
Grand Total (Part A+ Part B+ Part C)		
Grand Total in words		

SECTION-9 ANNEXURES & FORMATS

9.1 Annexure A Part 1 -Technical Specification for GIS Mapping of OFC Routes

The bidder must provide necessary details to BBNL/BSNL/USOF NOC regarding GIS mapping, following the format specified in the BSNL Amendment BharatNet Phase 3 RFP, as per the prior requirements of TENDERER. The bidder must thoroughly review the RFP and an indicative structure of the required data format outlined in this section, ensuring it includes but not limited to the following information:

1) Specification for GIS Mapping
2) Accuracy: Meter level accuracy (20 CM)
3) 50% collection of Lat/Long should be up to 1 Meters accuracy
4) 95% collection of Lat/Long should be up to 2 Meters accuracy.
5) Format: .SHP format with mapping on GCS projection system with WGS 84 datum.
6) Base Map for Validation: NIC Base map.
7) Codification and Layer structure will be provided by BBNL in amended BharatNet RFP. However, the shape files for OLT, ONT, Joints, Splitter, Route Indicators, OFC, FPOI (if existing fibre of BSNL is being used), Landmarks layers are to be prepared. Details of these layers are as given below:

OLT Layer			
Sr. No	**Field**	**Type**	**GPON Description**
1	Name	String	OLT Name
2	Type	String	Asset Type (OLT)
3	Asset_Code	String	OLT Code
4	NMSOLT_C D	String	NMS OLT Code
5	Blk_Name	String	Block Name
6	Blk_Code	String	Block Code
7	Dt_Name	String	District Name
8	Dt_Code	String	District Code
9	St_Name	String	State Name
10	St_Code	String	State Code
11	Lat	Double	Latitude
12	Long	Double	Longitude
13	Coil_Len	Double	Coil Length
14	Remarks	String	if any
15	Obs	String	Observation
16	Status	String	Editing Status/It should be blank
17	olt_ip	String	IP address of OLT

18	geo_photo	String	Photo with geo-location
19	Vendor	String	UTL,L&T,ITI,TEJAS
20	Phase	String	1
21	Model	String	BBNL/BSNL
22	Technology	String	GPON
ONT Layer			
Sr. No	**Field**	**Type**	**Description For GPON**
1	Name	String	ONT Name
2	Type	String	GP,BHQ
3	Asset_Code	String	ONT Code
4	LGD_Code	String	LGD Code for Location
5	Location	String	Location Name of ONT
6	Loc_Type	String	School, College, GP,PANCHAYAT BHAWAN etc
7	OLT_Code	String	OLT Code
8	NMSOLT_CD	String	NMS OLT Code
9	NMSONT_C D	String	NMS ONT Code
10	Blk_Name	String	Block Name
11	Blk_Code	String	Block Code
12	Dt_Name	String	District Name
13	Dt_Code	String	District Code
14	St_Name	String	State Name
15	St_Code	String	State Code
16	Lat	Double	Latitude
17	Long	Double	Longitude
18	Coil_Len	Double	Coil Length
19	Remarks	String	BBNL / BSNL Remarks
20	Obs	String	NIC Observations
21	Status	String	Editing Status/It should be blank
22	olt_ip	String	IP address of OLT
23	Ont_mac_id	String	Mac Id of ONT
24	Otdr_len	Double	Length in meters

25	Conn_str	String	PIC-PON-ONT ID
26	Ont_sr_no	String	Device serial no.
27	Olt_block	String	Block code of OLT
28	Backhaul	String	OFC or Sat
29	geo_photo	String	Photo with geo-location
30	Phase	String	1
31	Route_code	String	Incremental or leased
JOINT Layer			
Sr. No	**Field**	**Type**	**Description For GPON**
1	Name	String	Joint Name
2	Type	String	BJC/SJC
3	Asset_Code	String	Joint ID for NMS
4	Location	String	Location Name
5	Loc_Type	String	Location Type
6	OLT_code	String	OLT Code
7	Blk_Name	String	Block Name
8	Blk_Code	String	Block Code
9	Dt_Name	String	District Name
10	Dt_Code	String	District Code
11	St_Name	String	State Name
12	St_Code	String	State Code
13	Lat	Double	Latitude
14	Long	Double	Longitude
15	rd_Offset	Double	Offset from Middle of the Road
16	coil_2_ont	Double	Length Towards ONT
17	coil_2_olt	Double	Length Towards OLT
18	Remarks	String	BBNL / BSNL Remarks
19	Obs	String	NIC Observations
20	Status	String	Editing Status/ It should be blank
21	olt_ip	String	IP address of OLT
22	Otdr_len	Double	Length in meters
23	PHASE	String	1

24	Route_code	String	

JOINT Layer			
Sr. No	**Field**	**Type**	**Description For GPON**
1	Name	String	Joint Name
2	Type	String	BJC/SJC
3	Asset_Code	String	Joint ID for NMS
4	Location	String	Location Name
5	Loc_Type	String	Location Type
6	OLT_code	String	OLT Code
7	Blk_Name	String	Block Name
8	Blk_Code	String	Block Code
9	Dt_Name	String	District Name
10	Dt_Code	String	District Code
11	St_Name	String	State Name
12	St_Code	String	State Code
13	Lat	Double	Latitude
14	Long	Double	Longitude
15	rd_Offset	Double	Offset from Middle of the Road
16	coil_2_ont	Double	Length Towards ONT
17	coil_2_olt	Double	Length Towards OLT
18	Remarks	String	BBNL / BSNL Remarks
19	Obs	String	NIC Observations
20	Status	String	Editing Status/ It should be blank
21	olt_ip	String	IP address of OLT
22	Otdr_len	Double	Length in meters
23	PHASE	String	1
24	Route_code	String	

FPOI Layer			
Sr. No	**Field**	**Type**	**Description For GPON**
1	Name	String	FPOI Name
2	Location	String	Location Name
3	rd_Offset	Double	Offset from Middle of the Road

4	coil_2_ont	Double	Length Towards ONT
5	coil_2_olt	Double	Length Towards OLT
6	Lat	Double	Latitude
7	Long	Double	Longitude
8	Remarks	String	BBNL / BSNL Remarks
9	Type	String	Joint or Splitter
10	Blk_Code	String	Block Code
11	Blk_Name	String	Block Name
12	Dt_Code	String	District Code
13	Dt_Name	String	District Name
14	St_Code	String	State Code
15	St_Name	String	State Name
16	OLT_code	String	NIC OLT Code
17	Asset_Code	String	Joint/Splitter ID
18	Loc_type	String	School, College, GP, etc
19	fpoi_id	String	Id of FPOI
20	OTDR-Len/OTDR_Reading	String	PoN OTDR reading at FPOI from OLT
21	OLT_IP	String	IP Address of OLT connected to
22	Geo_photo	String	Photograph of FPOI with Geo-tagging
23	Obs	String	NIC Observations
Splitter Layer			
Sr. No	**Field**	**Type**	**Description**
1	Name	String	Splitter Name
2	Type	String	S2,S4,S8,S16
3	Asset_Code	String	Splitter ID
4	Location	String	Location Name
5	OLT_Code	String	NIC OLT Code
6	Blk_Name	String	Block Name
7	Blk_Code	String	Block Code
8	Dt_Name	String	District Name
9	Dt_Code	String	District Code
10	St_Name	String	State Name

11	St_Code	String	State Code
12	Lat	Double	Latitude
13	Long	Double	Longitude
14	rd_Offset	Double	Offset from Middle of the Road
15	coil_2_ont	Double	Length Towards ONT
16	coil_2_olt	Double	Length Towards OLT
17	Remarks	String	BBNL / BSNL Remarks
18	Obs	String	NIC Observations
19	Status	String	Editing Status/ It should be blank
20	geo_photo	String	Photo with geo-location
21	olt_ip	String	IP address of OLT
22	Otdr_len	Double	Length in meters
23	fiber_pos	String	Left/ Right of the road
24	Direction	String	Towards GP or Block
25	Phase	String	1
OFC Layer			
Sr. No	**Field**	**Type**	**Description**
1	Name	String	OFC Route name
2	Type	String	Leased/Incremental
3	Asset_Code	String	Segment Code
4	OLT_Code	String	OLT Code
5	Blk_Code	String	Block Code
6	Dt_Code	String	District Code
7	St_Code	String	State Code
8	CS	String	Cable Section
9	Seg_Length	Double	Route length
10	Start_Node	String	Starting Asset
11	S_Coil_Len	Double	Starting Coil Length
12	End_Node	String	Ending Asset
13	E_Coil_Len	Double	Ending Coil Length
14	num_fibre	String	6/12/24/48/96
15	Status	String	Editing Status/ It should be blank

16	Remarks	String	BBNL / BSNL Remarks
17	Obs	String	NIC Observations
18	Traverse	String	FIBRE POS‘T’ON e.g. 'U' For Un‘e’ground, 'O' for Overhead
19	fiber_pos	String	Left/ Right of the road
20	Direction	String	Towards GP or Block
21	Phase	String	1
22	Route_co de	String	Incremental or leased

RI			
Sr. No	**Field**	**Type**	**Description**
1	Name	String	RI NAME
2	Type	String	Asset Type
3	OLT_Code	String	OLT Code
4	Blk_Name	String	Block Name
5	Blk_Code	String	Block Code
6	Dt_Name	String	District Name
7	Dt_Code	String	District Code
8	St_Name	String	State Name
9	St_Code	String	State Code
10	Lat	Double	Latitude
11	Long	Double	Longitude
12	rd_Offset	Double	Offset from Centre of the Road
13	CS	String	Cable Section
14	Remarks	String	BBNL / BSNL Remarks
15	Obs	String	NIC Observations
16	coil_len	String	if any
17	Status	String	Editing Status/ It should be blank
18	geo_photo	String	Photo with geo-location
19	fiber_pos	String	Left/ Right of the road
20	direction	String	To wards GP or Block
21	Phase	String	1 or 2
22	Route_code	String	INCREMENTAL/LEASED

Landmark Layer			
Sr. No	**Field**	**Type**	**Description**
1	Name	String	Landmark Name
2	Type	String	Asset Type
3	OLT_NAME	String	OLT Name
4	OLT_Code	String	OLT Code
5	Blk_Name	String	Block Name
6	Blk_Code	String	Block Code
7	Dt_Name	String	District Name
8	Dt_Code	String	District Code
9	St_Name	String	State Name
10	St_Code	String	State Code
11	Lat	Double	Latitude
12	Long	Double	Longitude
13	Remarks	String	BBNL / BSNL Remarks
14	Obs	String	NIC Observations
15	Status	String	Editing Status/ It should be blank
16	geo_photo	String	Photo with geolocation
17	fiber_pos	String	Left/ Right of the road
18	Direction	String	Towards GP or Block
19	rd_offset	String	Offset from centre of the Road
20	Phase	String	1

1) Note: 1. Attributes in serial numbers with asterisk mark (*) will be provided by NIC or may be auto filled by the application.
2) Note: 2. Attributes in serial numbers with hash mark (#) will be used by application for processing, so need not to be filled.
3) Note: 3. All other fields are mandatory.
4) Note: 4. The information i.r.o. above tables, available with by BSNL/GFGNL will be provided.
5) Note:5. If any other layer is needed to be added, the same shall be intimated by GFGNL appropriately.
6) Codification and Layer structure will be provided by BBNL in amended Bharatnet RFP. However, the shape files for OLT, ONT, Joints, Splitter, Route Indicators, OFC, FPOI (if existing fibre of BSNL is being used), Landmarks layers are to be prepared. Details of these layers are as given below:
7) Uploading of geo tagged site images of designated locations of specified size e.g. 500

Kb. The Mobile App of BharatNet can also be used wherever required. Photos taken from site shall be optimized by the tool itself as per requirement.

8) Calibration: PON OTDR readings for calibration on each end of OLT, Splitter, Joint and ONT along with the coil length on each side to be done by bidder.

9) Interval of readings: The coordinates of landmarks like Culverts, Bridges / nallah, water bodies, cross roads, railway crossing, flyovers and public places like temples/mosques, bus-stop, PHC, Post office, School/College, shops, Police Stations, Banks, Tourist Spots, Hospitals, etc. to be captured along with the route indicators (RI), cable joints, splitter etc. along the cable routes. One additional reading in the middle of the two manholes / RI should be recorded in the already laid network. Recordings are necessarily to be made at every fibre turn, bend along the route, road/railway crossing, culverts, diversion etc. Sufficient recordings at short intervals on the curvature of the route shall be made such that it should be mapped on GIS properly.

10) Overhead or Underground alignment type of execution (HDD, OT, Aerial etc.)

11) Location of various assets like FPOI/SJC/BJC. OLT, ONT, Manholes, Joint Chambers, Splitter, FTBs FDMS route indicators etc. with geo tagged images

12) Count of terminated and spare fibres, loop, make and size of cable deployed, Optical test results for each fibre with the help of already recorded data by GFGNL and its fibre laying contractors. Port wise fibre built up and termination details. PON OTDR readings of FPOIs, Splitter and ONTs.

13) Route marker details: Cement/electronic Route Marker (Lat-Long) details Route Marker identification.

14) Road features: Length, width and type (RCC, Kuchha, pakka etc.). Variation in width of road in meters taking offset from the center of the road may be obtained from ABDs already available with BSNL.

15) Other operators/ utility: Presence of underground OFC of other operators, utility pipes, transmission cable etc. to be captured wherever possible.

16) RoW: Railway authority, NH, Forest authority and any other authority limits along with OFC path shall be obtained from existing ABDs available with BSNL.

17) For point feature like poles, Sewerage man holes, other utility chambers, transformers, bore well etc. shall be captured as a point.

18) For all utilities above ground viz. Poles, Manholes and telecom nodes like BTS and Telephone exchanges etc. details shall be recorded in a corridor of 50 m (25 m on either side of the road center line or ROW of road whichever is more).

19) To and/or from direction to village, town, city etc. shall be recorded for all roads.

20) The Geo Coordinates of all road KM stones shall be recorded and shown using symbol provided.

21) The Geo Coordinates of all property boundaries with in the corridor shall be recorded and shown in drawing.

22) Collection of data (Custodianship of GPON equipment, location of school, college, hotels, post office, other Govt. Offices, key contacts in GP etc.) in each Gram Panchayat and other important locations. Contact numbers of all the above Offices to be obtained.

- Note: All the asset location on ground is to geo-tagged in either five photographs (one close- up and four from different directions covering road part and also landmarks, if visible) OR to be captured or videography (zoom& wide angle) to be taken so as to identify the exact point later on. There will be a practical situation where the route indicators will be found missing. In such situation a play card with the notional assets

no. available RID/ABD to be placed on the identified point.

1. Process of uploading of GIS data and verification
2. Engineering Survey of GFGNL OLT location and routes from BSNL FPOI to respective ONTs in Gram Panchayats (GP) where cable is already laid or being laid.
3. Uploading of block wise / OLT wise data on GIS platform. BBNL/NIC shall provide base maps for uploading and optimizing the captured data and information including fibre built up and termination details.
4. Validation of uploaded data shall be done in three stages:
   a. First stage: The contractor shall upload and verify the block wise data in the tool.
   b. Second stage: Second level validation shall be done by BSNL/BBNL State units.
   c. Third Stage: Third level validation shall be done by BBNL/BSNL.
5. If the data correction is required at any of the stage mentioned above, the same may be sent to the previous stage for necessary correction. The contractor shall correct and upload the data again.
6. The contractor may edit/correct the data uploaded by them and submit for validation for next stage. After submission of data to next stage, the editing feature shall be freezed for contractor. The editing window shall be re-opened for contractor if some data correction is required at later stages.
7. Guidelines for data uploading and validation:

A) Registration of Users:

1. Contractor: The Contractor User is allotted a set of OLTs from a block and is allowed to edit the features only within those OLTs. The Contractor User is created by entering their details such as User Name, Password, Name, Address, E-Mail, selecting the State, District and Block from drop down lists, and by selecting the OLTs from a list within which he/she is allowed to edit.
2. GFGNL: GFGNL shall validate the data uploaded by the Contractor and after GFGNL approval the data shall be forwarded to GFGNL BA for next stage validation. GFGNL State Users shall be created by selecting the State from a drop down list and entering their other details.

B) Uploading and Editing of Data:

The editing module is available for the respective editing users, and the workflow of the module is as follows:

1. The editor will be prompted to select an OLT from a drop down list of all the OLTs that are allotted to that particular user.
2. Secondly, the user will choose any one of the following layers to upload, from a drop down list: OLT, ONT, Splitter, Joint, OFC, FPOI, RI and Landmark.
3. On selecting the layer for upload, the user can now upload a shape file using the upload form provided in the module.
4. On uploading the shape file, the data will be checked to see if the selected OLT has features in that particular layer based on OLT code, if there are features present, those features will be purged from the layer, and the newly uploaded data will be added to the layer.

C) As-Built Documentation:

ABD has to be prepared using two sets of information:

1. Physical OFC asset details and locations in respect of locations / asset visited for capturing GIS data during scope of work as this tender
2. Remaining data as per documentations / details made available to bidder w.r.t. to old PFC laid
3. The documentation consisting of the following shall be prepared Block to ONTs at Gram Panchayat based on the data collected for the GIS mapping. The As-Built shall be an essential part of the documentation process and shall ensure easy maintenance of the OFC route. This can be prepared using the existing RID/ABD/L-14/ MB/ PoN diagram etc. The 10 M reading can be captured from these documents. The OLT/ ONT/ FPOI/ Joint/ splitter/ RIs/ Landmark are being captured as point asset and OFC is being captured as line asset can be used for preparing this document. The As-built documentation shall be separately prepared for each Block.
4. The As-Built will contain the following details:
    1. Cable Details: Make and Size of the cable
    2. Joint Details:
        a) Location of Joint Chamber (Lat/ Long details in decimal degree format up to six-digit precision)
        b) Depth of Joint Chamber Cover from ground level
        c) Details of cable stack at each joint chamber
    3. Route Marker Details:
        a) Location of Route Marker Cement / Electronic (Lat/ Long details in decimal degree format up to six-digit precision)
        b) Route Marker Identification details
    4. OFC Alignment Details:
        a) Offset of cable from centre of the road at every 10 meter (Details to be captured from HDD Graph / Measurement book)
        b) Details of crossings (road / rail / nala etc) should be provided
        c) Depth profile of cable at every 10 Meter (Details to be captured from HDD Graph / Measurement Book
        d) Details of protection with type of protection (Details to be captured from GFGNL provided input)
        e) Locations of culvert and bridges with their lengths and scheme of laying of HDPE / PLB pipe thereon
    5. Landmark Details:
        a) Important landmarks to facilitate locating the cable position in future to include important buildings such hospital, religious places, petrol pumps, educational institutes, government offices, commercial complex, major residential complex / building etc
    6. Road Feature Details: Road feature to be captured as per below,
        i. Electric Pole / Transformer
        ii. Telephone Pole
        iii. Utility Manhole
        iv. KM Milestone

v. Street Pole / Lamp Post
vi. Median
vii. Utility Box
viii. Divider
ix. Large Tree

7. Readings should invariably be recorded at every bend on the road, road/railway crossings, culverts, diversion etc. at every 5 meters.
8. For all the linear features, geo coordinates shall be recorded at every turning point.
9. To and/or from direction to village, town, city etc. shall be recorded for all roads.
10. All the road KM stones shall be recorded and shown in drawing using symbol provided.
11. All the property boundaries with in the corridor shall be recorded and shown in drawing. Three point's references need to be shown for every joint chamber/Pull through Chamber/Manholes.
12. Collection of data (Custodianship of GPON equipment in each Gram Panchayat).
13. All the diagrams shall bear the signatures of the contractor and the project manager as a proof of accuracy of the details. The diagrams shall be bound in A- 3 size book with cover. The cover sheets shall be laminated and should have the following details.
    i. Name of the Project Organization.
    ii. Name of the OFC Link with ID.
    iii. Name of the Contractor.
    iv. Name of Survey Contractor Rep as part of Acceptance Test.
    v. Name of BSNL Rep as part of Acceptance Test.
    vi. Date of commencement of work.
    vii. Date of completion of work.
    viii. For each block 2 sets of documents shall be submitted.
14. RoW: Railway authority, National Highway, Forest Authority and any other authority limit along with OFC path shall be captured in the As-Built Map (Details will be provided in BSNL ancillary input data)
15. Submission of 'As Built Drawings (ABDs)' in GIS format (Shape Format) of OFC connectivity from Block OLT location to respective ONTs in Gram Panchayats (GP), Routes data in hard copy (A3 for grids) as well as soft copy. Each sheet shall record maximum 200 to 250 M of the route length.
16. BSNL shall provide on line tool for uploading the captured data and information.
17. As Built Drawings (ABDs) shall be uploaded in the GIS platform through on line tool provided by GFGNL in GIS format (Shape File, .shp).

9.2 Annexure A Part 2 -Scope of Work as per BharatNet ABP RFP

1. GIS data collection

- PIA of GFGNL ABP RFP shall conduct survey of the Block and associated routes from Block to Gram Panchayats (GPs) to evaluate the existing and new fiber cable needs for network implementation.
- PIA of GFGNL ABP RFP shall collect coordinates of landmarks such as culverts, bridges / nallah, water bodies, crossroads, railway crossing, flyovers and public places like temples/mosques, bus-stop, PHC, post office, school/college, shops, police stations, banks, tourist spots, hospitals, etc. to be captured along with the route marker, cable joints, etc. along with the cable routes. One additional reading in the middle of the two manholes / RI should be recorded in the already laid network. Recordings are necessarily to be made at every fibre turn, bend along the route, road/railway crossing, culverts, diversion etc. Sufficient recordings at short intervals on the curvature of the route shall be captured to map it on GIS properly.
- PIA of GFGNL ABP RFP shall collect photos of various assets such as Blocks, GPs, manholes, joint chambers, FDMS, route markers etc. with geo tagged images.
- PIA of GFGNL ABP RFP shall collect information about terminated and spare fibers, loops, cable types/sizes and optical test results for each fibre, utilizing previously recorded data from PH-I and PH-II. This includes port-by-port fibre configurations, termination details, and OTDR readings for Blocks and Gram Panchayats (GPs)
- PIA of GFGNL ABP RFP shall collect cement/electronic route marker (Lat-long) details for route marker identification.
- PIA of GFGNL ABP RFP shall collect information about road length, width and type (RCC etc.). variation in width of road in meters taking offset from the center of the road.
- PIA of GFGNL ABP RFP shall gather details about authorities such as railway, National Highways (NH) and forest departments within the limits of the OFC path required for RoW permissions.
- The point feature like poles, sewerage manholes, other utility chambers, transformers, bore well etc. shall be captured as a point.
- The record of Block, GP and any utility shall be maintained within a 50-meter corridor with an accuracy of 20 cm (25 meters on each side of the road's center line or within the road's right-of-way, whichever is greater)
- To and fro direction towards village, town, city etc. shall be recorded for all roads.
- The geo coordinates of all road KM stones shall be recorded and shown using symbol provided.

Note: All the asset locations on ground are to be geo-tagged in five photographs (one close-up and four from different directions covering road part and also landmarks, if visible) and videography (zoom & wide angle) to be taken so as to identify the exact point later on. There will be a practical situation where the route markers will be found missing, in such situation a play card with the notional assets no. available RID/ABD to be placed on the identified point.

2. Mobile app for data collection from field

PIA of GFGNL ABP RFP shall use mobile application & video recording solution for the BharatNet Project to accurately document project activities such as trenching, fibre laying, splicing and equipment deployment. The key requirements are given below.

- PIA of GFGNL ABP RFP shall record videos of depth, offset, chainage marking, etc. of overhead or underground alignment type of execution (HDD, OT, Aerial etc.)
- The video should support to record and identify depth, offset, ofc accessories details and landmarks of routes.
- PIA of GFGNL ABP RFP shall ensure that the accuracy of videos and GIS coordinates is within the range of 20 cm. (a sample check of the survey shall be performed on the ground by GFGNL Representative/Bidder resource to check the Submeter level accuracy (≤ 20 centimeters). GFGNL may use CORS system deployed by Survey of India for measuring the accuracy during sample check. The survey data shall be rejected if the accuracy of the sample data is not in accordance with the desired accuracy).
- The PIA of GFGNL ABP RFP should use suitable devices such as GNSS / DGPS (which can be pole-mounted or handheld as necessary), or any other appropriate technology and mobile applications for conducting surveys to capture GIS coordinates, videos, and photos of completed work.
- The mobile app provided by GIS bidder can be used as needed for capturing GIS coordinates, videos, and photos of executed work. The GNSS/ DGPS or any other device used by the PIA of GFGNL ABP RFP must be compatible with the mobile app. If the PIA opts for its own application than PIA shall upload videos in mp4 format and GIS coordinates in shape file format on BSNL provided GIS application. If the PIA uses the GFGNL mobile app, videos and GIS coordinates will be uploaded automatically.
- If PIA used own mobile app, in such case all videos and photos shall be geo tagged and geo location shall be mentioned in file name. The geographical information shall also be available in header file.

3. Video specifications:

- Format: MP4 format, minimum 720p & and above resolution, and 30 fps/60fps frame rate with HEVC codec for video compression.
- Content: Each video segment shall clearly capture start and end points of activities, depth readings for trenching/drilling, manhole/cable chamber installation, details of OFC blowing/pulling, splicing activities, route markers, and active equipment deployment procedures.
- Continuous recording: Videos shall be recorded continuously without cuts or edits, and file sizes should be optimized for efficient data exchange.
- Visual evidence: Use calibrated vertical measuring tools to display depth in the video frame at every 10 meters for Open Trenching.
- Verbal commentary: Provide running commentary describing activities, depth measurements, and location references.
- Date and time stamp: Automatically embed date and time stamps in recordings.
- File naming: File names should clearly indicate the type of work, block, and route.
- The following details (indicative) shall be captured in videos:
    i. Chainage (CH) details
    ii. Methodology type
    iii. Depth and Offset details.
    iv. Lat long of each pit, RI, splice chamber landmarks etc.
    v. Crossing of roads

vi. 3 reference points of RI, Block and GP

vii. Major crossing

viii. Forest area, etc.

Note:

- Requirements for mobile device/ handset for GIS mobile app
- The PIA shall have dedicated mobile for BharatNet program to capture implementation videos.
- Mobile device shall support minimum android version 13.0 & iOS version 15 for operating the GIS mobile application.
- Mobile device shall support minimum camera capacity of 48 MP or higher and have at least 256 GB storage with augmented cloud storage capabilities as well.
- The camera should provide stable footage with minimal shaking or distortion.
- The video recording needs to be captured in sufficient day light and significant speed of maximum 40mtr/minute and minimum of 20mtr/minute.
- The video recorded and uploaded by PIA to BSNL shall also be stored by the PIA for future reference, extending for a duration of one year or until invoicing, whichever is higher.
- Mobile device shall support all the required features to fulfill the video recording requirements as given in tech specs of GIS Data upload and validation clause no 3

4. GIS data upload and validation

- Bidder shall provide online tool and measurement book format for uploading the captured data and information.
- The PIA of GFGNL ABP RFP shall upload geotagged images and videos of designated locations in specified formats given in clause 2.4 below. The mobile app of BharatNet shall be used to upload photos and videos to be taken from the sites.
- To upload Block-wise data on GIS application (web and mobile), Bidder of this RFP will provide base maps to facilitate the upload and optimization of captured data and information, including fibre infrastructure and termination details etc.
- Validation of uploaded data shall be done in two stages:
    a) **First stage:** The PIA shall upload and verify the Block wise data/ videos/ photos in the GIS application (web/ mobile)
    b) **Second stage:** Second level validation shall be done by GFGNL representative of respective Block /bidder resource.
- If the data correction is required at any stage, the same shall be sent to the PIA for necessary correction.
- PIA shall be responsible to modify/ correct the data and submit for revalidation by the GFGNL.

5. Digital As-Built Drawing (ABD):

- As-Built Drawing (ABD) shall be created digitally on GIS platform.
- The PIA of GFGNL ABP RFP shall record details of other operators and utilities such as underground optical fiber cables, utility pipes, transmission cables, and other similar infrastructure, in the digital ABD wherever possible.
- The geo coordinates of all property boundaries within the fibre route corridor shall be

recorded and shown in digital ABD.

- The PIA of GFGNL ABP RFP shall capture physical OFC asset details and locations in respect of locations/ asset visited for capturing GIS data during scope of work as mentioned in this tender.
- Existing data as per documentations/ details made available to The PIA of GFGNL ABP RFP w.r.t. to old OFC laid.
- ABD shall be prepared from Block to GPs during implementation. The ABD for each block shall be prepared separately. ABD may have the following details:

Particulars	Parameters to be captured (indicative)
Cable details	• Make and Size of the cable
Joint details	• Location of Joint Chamber (Lat/ Long details in decimal degree format up to six-digit precision) • Depth of Joint Chamber Cover from ground level • Details of cable stack at each joint chamber • 3 reference point of joint locations
Route marker	• Location of Route Marker Cement / Electronic (Lat/ Long details in decimal degree format up to six-digit precision) • Route Marker Identification details • 3 reference point of each route marker
OFC Alignment Details	• Offset of cable from centre of the road at every 10 meters (Details to be captured from HDD Graph / digital measurement book) • Details of crossings (road / rail / nala etc) should be provided. • Depth profile of cable at every 10 Meter (Details to be captured from HDD Graph / Measurement Book • Details of protection with type of protection (Details to be captured from BSNL provided input) • Locations of culvert and bridges with their lengths and scheme of laying of HDPE / PLB pipe thereon
Landmark Details	• Important landmarks to facilitate locating the cable position in future to include important buildings such hospital, religious places, petrol pumps, educational institutes, government offices, commercial complex, major residential complex / building etc
Road feature details	• Electric Pole / Transformer • Telephone Pole • Utility Manhole • KM Milestone • Street Pole / Lamp Post • Median

Particulars	Parameters to be captured (indicative)
	• Divider • Large Tree

- Readings shall be recorded without any exception at interval of 10 meters including every bend on the road, road/railway crossings, culverts, diversion etc. Each section shall record maximum 200 to 250 meter of the route length.
- All the property boundaries within the corridor shall be recorded and shown in drawing. Three point's references need to be shown for every joint chamber/pull through chamber/manholes.
- Collection of data shall also include custodianship of equipment in each Gram Panchayat.
- All the diagrams shall be verified by the PIA (project manager level person) as a proof of accuracy of the details. The ABD may have the following details.
  i. Name of the Project Organization
  ii. Name of the OFC Link with ID
  iii. Name of the PIA
  iv. Name of Survey PIA Rep as part of acceptance test
  v. Name of BSNL Rep (IE) as part of acceptance test
  vi. Date of commencement of work.
  vii. Date of completion of work
- RoW: Railway authority, National highway, Forest authority and any other authority limit along with OFC path shall be captured in ABD.
- The The PIA of GFGNL ABP RFP shall also be provided option to upload ABD in GIS format (.shp etc.) in the GIS platform through online tool to be provided by bidder. In such cases, The PIA of GFGNL ABP RFP shall prepare ABD in GIS format (shape format) of OFC connectivity from Block location to respective Gram Panchayats (GPs), routes data shall be in soft copy.

6. Functional requirements for PM tool

The project monitoring tool shall enable real-time tracking of project progress, (timelines and milestones) including the status of network infrastructure deployment, equipment installation, and connectivity establishment across all packages of Amended BharatNet program.

1 The PIA of GFGNL ABP RFP shall provide the input for managing project documents, drawings, specifications, permits, contracts, and other relevant documentation etc.

2 The PIA of GFGNL ABP RFP shall provide all required information for the application dashboard in standard/ defined format such as measurement book, acceptance test proofs etc. The details shall be, but not restricted to, as under: -

- Block/GP wise Cable Length.
- Block /GP wise Duct length.
- Block /GP wise Trench Length.
- Total as build OSP network elements count/details of FDMS/ Handhole/ Manhole/ Site/ Splice Closure etc.

- Total Planned OSP network elements count/details of FDMS/ Handhole/ Manhole/ Router/ Site/Splice Closure etc.
- Total ISP network Elements count/details of Router/ Switch/OLT /Repeater /Equipment's etc.

3 The PIA of GFGNL ABP RFP shall be responsible to update the project progress in the project monitoring tool, enabling the system to automatically create milestone-based proforma invoices.

7. Digital measurement book

- Digital measurement book module of BharatNet S-S-NOC and C-S-NOC shall automatically calculate and update the work completed data including route length in RKM, depth etc. based on the videos uploaded during the execution of the work.
- PIA shall be responsible to provide/ update the measurement book information in the PM tool MB module via mobile application to record work details in the S-S-NOC and C-S-NOC MB module if required. The recorded, reading in the MB cannot be deleted. The MB data shall be validated by the (approved/ rejected) by the IE. PIA shall maintain and store all details of measurement book till the completion of C-S-NOC application. After completion of C-S-NOC, PIA shall upload all required data in PM tool.
- PIA shall also get an option for manual entry of records in digital measurement book of PM tool in case of any issue faced in automated process.

8. Inspection and audit module

PIA shall have access of PM tool inspection and audit module, this module shall be utilized by IE to validate the high- and low-level network design, inspect the project and identify any lapses/defect etc. The PIA shall provide comments on the observations and describe the necessary actions required, including specific timelines for completion.

9.3 Annexure B- Existing S-NOC infra

Sr. No	Item	Make and Model	Unit
1	55inch Full HD LED Video wall Display panel with Extreme Narrow Bezel(1.7mm)	Christie FHD-5S3XE (5x3 mat	15
2	Wall Mount Bracket for above video wall display	Branded	15
3	Video wall controller with 16HDMl input and 24HDM1 output and Video wall management software	Datapath VSN1172-RPSU	1
4	HDMI cable (50mtrs)	Kramer CLS-AOCH/60-164	30
5	LIU - 48 Port X 2	Norden	
6	Fortinet FIREWALL 24 Port		
7	Multiple WAN Router	Cisco	
8	LAN POE switch - 24 PORT X 2	Allied Telesys	2
9	WIRELESS AP	Netgear	
10	CAT6 UTP Cable (305mtrs)	Norden	4
11	CAT6 Patch Panel 24port	Norden	
12	CAT6 Patch Cord (1Mtrs)	Norden	48
13	CAT6 Patch Cord (2Mtrs)	Norden	48
14	CAT61/0 Faceplate and Back box	Norden	48
15	Rack mountable PC with 22inch Monitor , Keyboard and Mouse.	Advantech	
16	42U Rack with two vertical PDU	Valrack	
17	OFC Termination at	OTS	96
18	Installation and commissioning charges	OTS	

Furniture:

Sr. No	Material Description	Size	Qty	Unit
1	Operator Desk 1	750 x 4500 x 750	3	Nos
2	Operator Desk 2	7500 x 3500 x 750	3	Nos
3	Chairs	-	15	Nos
4	Desktop	-	15	Nos

UPS:

Sr. No.	Material Description	Qty.	Unit
1	Supply, installation & Commissioning of Arrow 20 KVA online UPS with 2 Hours battery backup with 1 year onsite warranty including Battery.	1	Nos.

9.4 Check list

Sr. No	Documents to be submitted	Submitted (Y / N)	Documentary Proof (Page No.)
Qualification Criteria			
1	Demand Draft as bid processing fee		
2	EMD as Bid Security (DD/ BG as per Annexure V)		
Technical Qualification			
3	Cover Letter (Annexure I)		
4	Bidder's information sheet (Annexure II)		
5	Enclose copy of Certificate of Incorporation/ Registration Certificate of the firm certificate		
6	Copy of Certificate from the Statutory auditor/CA clearly specifying the annual turnover for the specified years. (2019-2020, 2020-21, 2021-22 & 2022-23).		
7	A copy of the OEM Partner Certification must be submitted		
8	Copies of Purchase Order (s) having executed the similar orders in last three years (from date of Bid) to be enclosed along with Technical Bid		
9	MAF issued by OEM for the proposed product as per format mentioned in Annexure -VIII		
10	Acknowledgement/ Copies of Income tax refund (ITR) filed for last three financial years i.e. 2019-2020, 2020-21, 2021-22 & 2022-23		
11	Copy of Certificate of Registration /Copy of certificate of incorporation / partnership deed (if applicable)		
12	Copy of valid GST registration		
13	Copy of valid PAN card		
14	Undertaking by the bidder for not being barred by any State/ Central Government/PSU (Annexure IV)		
15	Un-Priced BOM		

Sr. No	Documents to be submitted	Submitted (Y / N)	Documentary Proof (Page No.)
16	Annexure IX,X,XI,XII,XIII		
Financial Proposal			
17	Annexure VII Online		
18	Priced Detailed BOM Physically		

9.5 Format I

Proposal Covering Letter

(To be on the Bidder's letterhead duly Signed by Authorized Signatory)

Tender Ref No:

To
Chief Finance Officer (CFO)
Gujarat Fibre Grid Network Limited (GFGNL),
Block No: 6, 5th Floor,
Udyog Bhavan,
Sector-11, Gandhinagar -382010

Ref: RFP FOR UPGRADE OF NETWORK OPERATION CENTER-GFGNL ---------- ------- for a period of 7 Years + 3 years extendable

Dear Sir,

We …… (Name of the bidder) hereby submit our proposal in response to notice inviting tender document no. xxxxxxxxxx Dated: xx.xx.xxxx and confirm that:

1. All information provided in this proposal and in the attachments, is true and correct to the best of our knowledge and belief.
2. We shall make available any additional information if required to verify the correctness of the above statement.
3. Certified that the period of validity of bids is 180 days from the last date of submission of proposal, and
4. We are quoting for all the items (including services) as per the price bid format as mentioned in the RFP.
5. We the Bidder are not under a declaration of Ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government agencies.
6. We have an office in the state and relevant documents for the same are attached. We undertake that if the local presence is not there in the state, that we shall establish an office at Gandhinagar/ Ahmedabad, within 45 days from the date of the award of contract.
7. Gujarat Fibre Grid Network Limited (GFGNL) may contact the following person for further Information regarding this tender:
    a. Name & Designation:
    b. Full address of office
    c. Email ID & Contact No.
8. We are uploading our Response to the RFP (Eligibility, technical and financial bid documents) as per the instructions set out in this RFP.

Yours Sincerely,

(Signature)

Name of Authorized Signatory:
Designation:
Date:
Name of the bidder:

9.6 Format II

Format for Power of Attorney

(To be provided in original on stamp paper of value required under law duly Signed by 'bidder'**)**

Dated:

POWER OF ATTORNEY

To Whomsoever It May Concern

Know all men by these presents, we (Name and registered office address of the Bidder) do hereby constitute, appoint and authorize (Name of the Person(s)), domiciled at Mr./Ms./Mrs. _____ (Address), acting as (Designation and the name of the firm), as Authorized Signatory and whose Signature is attested below, as our attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for award of Contract "RFP FOR UPGRADE OF NETWORK OPERATION CENTER-GFGNL ---------- for a period of 7 Years+ 3 years extendable " , vide RFP (Tender Document) Document No._____dated _____ , issued by Gujarat Fibre Grid Network Limited (GFGNL), including Signing and submission of all documents and providing information and responses to clarifications / enquiries etc. as may be required by Gujarat Fibre Grid Network Limited (GFGNL) or any governmental authority, representing us in all matters before Gujarat Fibre Grid Network Limited (GFGNL), and generally dealing with GFGNL in all matters in connection with our Proposal for the said Project. We hereby agree to ratify all acts, deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all acts, deeds and things done by our aforesaid attorney shall and shall always be deemed to have been done by us.

For .....
(Signature)
(Name, Title and Address)
Accept (Attested Signature of Mr./Ms./Mrs._____
(Name, Title and Address of the Attorney)

Notes: To be executed by the Bidder - The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure. - Also, wherever required, the executant(s) should submit for verification the extract of the charter documents and documents such as a resolution / power of attorney in favour of the Person executing this Power of Attorney for the delegation of power hereunder on behalf of the executants(s).

9.7 Format III

Bank Guarantee format for Earnest Money Deposit

Date:

To
Chief Finance Officer (CFO)
Gujarat Fibre Grid Network Limited (GFGNL),
Block No: 6, 5th Floor,
Udyog Bhavan,
Sector-11, Gandhinagar -382010

Whereas ---------- (here in after called "the Bidder") has submitted its bid dated ---------- in response to the Tender no: xxxxxxxxxxxxxxxxxx for _____ KNOW ALL MEN by these presents that WE having our registered office at -- (hereinafter called "the Bank") are bound unto the___, Gujarat Fibre Grid Network Limited in the sum of for which payment well and truly to be made to Gujarat Fibre Grid Network Limited (GFGNL) , the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ---------

-----day of --2025.

THE CONDITIONS of this obligation are:

The EMD may be forfeited, In case of a Bidder if:

1) The bidder withdraws its bid during the period of bid validity.
    a. The Bidder does not respond to requests for clarification of their Bid.
    b. The Bidder fails to co-operate in the Bid evaluation process.
    c. The bidder, fails to furnish Performance Bank Guarantee in time.
2) The bidder fails to Sign the contract in accordance with this RFP
3) The bidder is found to be involved in fraudulent and corrupt practices

We undertake to pay to the GFGNL up to the above amount upon receipt of its first written demand, without GFGNL having to substantiate its demand, provided that in its demand GFGNL will specify that the amount claimed by it is due to it owing to the occurrence of any of the above-mentioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to 6 months from the last date of bid submission. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the GFGNL and further agrees that the guarantee herein contained shall continue to be enforceable till the GFGNL discharges this guarantee The

Bank shall not be released of its obligations under these presents by any exercise by the GFGNL of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the GFGNL or any other indulgence shown by the GFGNL or by any other matter or things.

The Bank also agree that the GFGNL at its option shall be entitled to enforce this

Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the TENDERER may have in relation to the SELLER's liabilities.

Dated at_____on this_____day of

_____2025. Signed and delivered by

_____

For & on Behalf of
Name of the Bank &
Branch & Its official
Address with seal

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the
G.R. no. EMD/10/2020/42/DMO dated 19.10.2020 issued by Finance Department or further instruction issued by Finance department time to time.

9.8 Format IV

PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref: Bank Guarantee No.

Date:

To
Chief Finance Officer (CFO)
Gujarat Fibre Grid Network Limited (GFGNL),
Block No: 6, 5th Floor,
Udyog Bhavan,
Sector-11, Gandhinagar -382010

Dear Sir,

WHEREAS..... (Name of Bidder) hereinafter called “the Bidder" has undertaken, in pursuance of Agreement dated, (hereinafter referred to as "the Agreement for “RFP for selection of Service Partner for providing ---------- for a period of ------ Years ***(Tender No. xxxxxxxxxxxxxxxx Dated: xx.xx.xxxx)*** for the Department of Science & Technology, Government of Gujarat.

AND WHEREAS it has been stipulated in the said Agreement that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.

1.WHEREAS we____("the Bank", which expression shall be deemed to include it successors and permitted as Signs) have agreed to give the Gujarat Fibre Grid Network Limited ("GFGNL") the Guarantee:

THEREFORE, the Bank hereby agrees and affirms as follows:

The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to GFGNL under the terms of their Agreement dated_____.

Provided, however, that the maximum liability of the Bank towards GFGNL under this Guarantee shall not, under any circumstances, exceed

_____ in aggregate.

2.In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from GFGNL in that behalf and without delay/demur or set off, pay to GFGNL any and all sums demanded by GFGNL under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from GFGNL to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:

_____
_____
_____

Attention Mr._____.

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of months from the date of its execution. The Bank shall extend the Guarantee for a further period which may be mutually decided by the bidder and GFGNL.

The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged, or otherwise affected by:

- Any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.
- Any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or Future, between Bidder and the Bank.
-

4. The BANK also agrees that GFGNL at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the BIDDER and not withstanding any security or other guarantee that GFGNL may have in relation to the Bidder's liabilities.

5. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of GFGNL or any other indulgence shown by GFGNL or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.

6. This Guarantee shall be governed by the laws of India and the courts of Gandhinagar shall have jurisdiction in the adjudication of any dispute which may arise hereunder.

Dated this ……. Day of ,2025

Witness

(Signature)
(Name)

(Official Address)

(Signature)
Bank Rubber Stamp
(Name)
Designation with Bank Stamp
Plus, Attorney as per Power
of Attorney No.

Dated:

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Urban Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no.

EMD/10/2020/42/DMO dated 19.10.2020 issued by Finance Department or further instruction issued by Finance department time to time.

9.9 Format V

Earnest Money Deposit Details

Sr. No.	Item	Amount (In Rs.)	Name of the Bank & Branch	Demand Draft No.
1	**Earnest Money Deposit (E.M.D.)**			

Eligibility Criteria

Form No. A: Company Registration

Sr. No	Name of Bidder	Certificate of Incorporation	Document Submitted or Not?
1			

Note: Please fill this form and upload the supporting documents.

Form No. B:Office in GUJARAT

Sr. No.	Address	Contact Person	Contact Nos.	Type of supporting document attached
1				

Note: You may mention more than one office (if applicable) by adding multiple rows which may be added by "NUMBER OF ROWS TO ADD".

Form No. C:Work Experience

Sr. No.	Project	Project Details	Period of Contract	Contact details of client	Type of supporting document attached
1					

Note: You may mention more than one project by adding multiple rows which may be added by "NUMBER OF ROWS TO ADD".

Financial Details of the Bidder

Turnover (INR: In Crores)		
2020 – 21	**2021 – 22**	**2022-23**

Note:

1. Submit the audited financial statement/ audited annual report of the above-mentioned financial years.

Name:
Designation:
Signature of the Authorized Signatory (with seal):

9.10 Format VI

Performa of Compliance Letter

(Submit copy on Bidder's letterhead duly signed by Authorized signatory) Date: *dd /mm /yyyy*

To
Chief Finance Officer (CFO)
Gujarat Fibre Grid Network Limited (GFGNL),
Block No: 6, 5th Floor,
Udyog Bhavan,
Sector-11, Gandhinagar -382010

Sub.: Compliance with the tender terms and conditions, specifications and Eligibility Criteria.

Dear Sir,

With reference to above referred tender, I, undersigned <<Name of Signatory>>, in the capacity of <<*Designation of Signatory*>>, is authorized to give the undertaking on behalf of <<*Name of the bidder*>>. We have to inform you that we have read and understood the technical specifications and total requirements of the above-mentioned bid submitted by us on <<*Date*>>. We hereby confirm that all our quoted items meet or exceed the requirements and are absolutely compliant with specifications mentioned in the bid document.

We also explicitly understand that all quoted items meet technical specifications of the bid and that such technical specifications override the brochures/standard literature if the same contradict or not indicated in brochures.

We are not banned or blacklisted by any Government institution of India.

In case of breach of any of the terms and conditions of the tender or deviation from bid specifications other than already specified as mentioned above, the decision of GFGNL Tender Committee for disqualification will be final and accepted by us.

Thanking you,

For <Name of the bidder>>
<<Authorized Signatory>>
<<Stamp of the bidder>>

9.11 Format VII

Declaration Letter

Physical submission on Company's letter head.

Date : <<dd-mm-yyyy>> To,

To
Chief Finance Officer (CFO)
Gujarat Fibre Grid Network Limited (GFGNL),
Block No: 6, 5th Floor,
Udyog Bhavan,
Sector-11, Gandhinagar -382010

Subject: DECLARATION OF NOT BANNED/BLACKLISTED/DEBARRED

Dear Sir,

With reference to the tender "<<*Tender Name*>>", I, undersigned <<*Name of Signatory*>>, in the capacity of <<*Designation of Signatory*>> certify that, our Company <<*Name of the bidder*>> is not banned or blacklisted or debarred by any Central/State Government Authority/Institution.

Signature: _____
Name: _____
Designation: _____
Name of the Company: _
Date:_____/_____/_____.
Place:_____.

9.12 Format VIII

On letterhead of Bidder/ESP/OEM

Undertaking as per guidelines published by Ministry of Finance, Dept. of Expenditure, Public Procurement division dated 23.07.2020.

Mr._undersigned authorized representative of M/s <<*Name of Bidder/ESP/OEM*>> has read clause regarding restriction on procurement from a bidder of a country which shares a land border with India; I certify that <<Name of Bidder/ESP/OEM>> is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that <<Name of Bidder/ESP/OEM>> fulfills all requirements in this regard and eligible to be considered. [Where applicable, evidence of valid registration by Competent Authority shall be attached.]

If given information is found to be false, this would be ground for immediate termination and further legal action in accordance with law.

(Signature)

Authorized representative of <<Name of Bidder/ESP/OEM>>

9.13 Format IX

Format of MAF/OEM Authorization

No._____dated _____

To

_____
_____
_____

Ref: Tender No. _____

Subject: _____

Dear Sir,

We, _____ who are established and reputed developers/manufacturers of _____ having development center/ factories at _____ _____(address of development center/factory) do hereby authorize M/s. _____

_____(Name & Address of agent) to submit a bid and sign the contract with you against above mentioned RFP.

We authorized the_____(name of the bidder) for the following modules/products:

Sr. No.	Product Name	Make & Model

<<for components>>

We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty and support including subscription covering upgrades, updates, patch updates, bug fixes, Fault Reporting, Trouble Ticketing, call resolution etc. available for the period of two years for the entire scope of the project through M/s_____(SI/ Bidder) from the date of Go-Live and also till Go-live.

<<For Hardware components>>

We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back-to-back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of two years for the entire

scope of the project through M/s_____
(SI/ Bidder) from the date of Go-Live and also till Go-live.

Yours

faithfully,

(Name)
(Name of manufacturers)
_____