

Bid Document

Bid Details	
Bid End Date/Time	12-10-2022 14:00:00
Bid Opening Date/Time	12-10-2022 14:30:00
Bid Offer Validity (From End Date)	75 (Days)
Ministry/State Name	Ministry Of Electronics And Information Technology
Department Name	Na
Organisation Name	Education And Research Network (ernet)
Office Name	East Zone
Total Quantity	1
Item Category	Selection of System Integrator for Supply and Setting up of ICT Infrastructure at DC and Remote (Q3)
MSE Exemption for Years of Experience and Turnover	No
Startup Exemption for Years of Experience and Turnover	No
Document required from seller	Experience Criteria,Past Performance,Bidder Turnover,Certificate (Requested in ATC),OEM Authorization Certificate,OEM Annual Turnover,Additional Doc 1 (Requested in ATC),Additional Doc 2 (Requested in ATC),Additional Doc 3 (Requested in ATC),Additional Doc 4 (Requested in ATC),Compliance of BoQ specification and supporting document *In case any bidder is seeking exemption from Experience / Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer
Past Performance	40 %
Bid to RA enabled	Yes
RA Qualification Rule	H1-Highest Priced Bid Elimination
RCM Applicable	Yes
Time allowed for Technical Clarifications during technical evaluation	5 Days
Evaluation Method	Total value wise evaluation

EMD Detail

Required	No
----------	----

ePBG Detail

Advisory Bank	Bank of India
ePBG Percentage(%)	3.00
Duration of ePBG required (Months).	46

(a). EMD & Performance security should be in favour of Beneficiary, wherever it is applicable.

Beneficiary:

Section Officer
East Zone, NA, Education and Research Network (ERNET), Ministry of Electronics and Information Technology
(Anju Rakheja)

Splitting

Bid splitting not applied.

MSE Purchase Preference

MSE Purchase Preference	No
-------------------------	----

Details of the Competent Authority for MSE

Name of Competent Authority	Sanjeev Banzal
Designation of Competent Authority	DG, ERNET India
Office / Department / Division of Competent Authority	ERNET India
CA Approval Number	
Competent Authority Approval Date	12-09-2022
Brief Description of the Approval Granted by Competent Authority	No relaxation granted to MSE by Competent Authority as the project is of very high value and experience system integrator is required to deliver the project.

Competent Authority Approval for not opting Micro and Small Enterprises Preference : [View Document](#)

MII Purchase Preference

MII Purchase Preference	Yes
-------------------------	-----

1. Preference to Make In India products (For bids > 200 Crore) (can also be used in Bids < 200 Crore but only after exemption by competent authority as defined in Deptt of Expenditure OM dated 28.5.2020): Preference shall be given to Class 1 local supplier as defined in public procurement (Preference to Make in India), Order 2017 as amended from time to time and its subsequent Orders/Notifications issued by concerned Nodal Ministry for specific Goods/Products. The minimum local content to qualify as a Class 1 local supplier is denoted in the bid document. If the bidder wants to avail the Purchase preference, the bidder must upload a certificate from the OEM regarding the percentage of the local content and the details of locations at which the local value addition is made along with their bid, failing which no purchase preference shall be granted. In case the bid value is more than Rs 10 Crore, the declaration relating to percentage of local content shall be certified by the statutory auditor

or cost auditor, if the OEM is a company and by a practicing cost accountant or a chartered accountant for OEMs other than companies as per the Public Procurement (preference to Make-in -India) order 2017 dated 04.06.2020. In case Buyer has selected Purchase preference to Micro and Small Enterprises clause in the bid, the same will get precedence over this clause.

2. Past Performance: The Bidder or its OEM {themselves or through re-seller(s)} should have supplied same or similar Category Products for 40% of bid quantity, in at least one of the last three Financial years before the bid opening date to any Central / State Govt Organization / PSU / Public Listed Company. Copies of relevant contracts (proving supply of cumulative order quantity in any one financial year) to be submitted along with bid in support of quantity supplied in the relevant Financial year. In case of bunch bids, the category related to primary product having highest bid value should meet this criterion.

Section 9(3) Of GST

Where ever RCM is applicable, sellers (Regular GST registered seller who opted out of FCM , unregistered seller, seller registered under composition scheme)will be forced to put Zero GST and GST cess in their bids. Buyer will have liability of paying the GST and GST cess to the government on the specified rate mentioned by them in this Bid.

3. Reverse Auction would be conducted amongst all the technically qualified bidders except the Highest quoting bidder. The technically qualified Highest Quoting bidder will not be allowed to participate in RA. However, H-1 will also be allowed to participate in RA in following cases:

- i. If number of technically qualified bidders are only 2 or 3.
- ii. If Buyer has chosen to split the bid amongst N sellers, and H1 bid is coming within N.
- iii. In case Primary product of only one OEM is left in contention for participation in RA on elimination of H-1.
- iv. If L-1 is non-MSE and H-1 is eligible MSE and H-1 price is coming within price band of 15% of Non-MSE L-1
- v. If L-1 is non-MII and H-1 is eligible MII and H-1 price is coming within price band of 20% of Non-MII L-1

Pre Bid Detail(s)

Pre-Bid Date and Time	Pre-Bid Venue
27-09-2022 14:00:00	Prebid meeting will be held online. Meeting link will be shared on 26.09.2022 on ERNET's website "https://ernet.in/tender".

Selection Of System Integrator For Supply And Setting Up Of ICT Infrastructure At DC And Remote (1 pieces)

(Minimum 50% and 20% Local Content required for qualifying as Class 1 and Class 2 Local Supplier respectively)

Brand Type	Unbranded
------------	-----------

Technical Specifications

Buyer Specification Document	Download
------------------------------	--------------------------

Input Tax Credit(ITC) and Reverse Charge(RCM) Details

ITC on GST	ITC on GST Cess	RCM Applicable	GST as per RCM	GST Cess 1 as per RCM	GST Cess 2 as per RCM	Optional RCM
NA	NA	Yes	18%	NA	NA	Yes

Consignees/Reporting Officer and Quantity

S.No.	Consignee/Reporting Officer	Address	Quantity	Delivery Days
1	Anju Rakheja	110053,ERNET INDIA 5 TH FLOOR BLOCK1,A WING DMRC, IT PARK SHASTRI PARK, DELHI PIN-110053	1	112

Buyer added Bid Specific Additional Scope of Work

S.No.	Document Title	Description	Applicable i.r.o. Items
1	Selection of System Integrator for Supply and Setting up of ICT Infrastructure at Data Centres and Remote Sites and Operation & Maintenance View	Selection of System Integrator for Supply and Setting up of ICT Infrastructure at Data Centres and Remote Sites and Operation & Maintenance	Selection Of System Integrator For Supply And Setting Up Of ICT Infrastructure At DC And Remote(1)

The uploaded document only contains Buyer specific Additional Scope of Work and / or Drawings for the bid items added with due approval of Buyer's competent authority. Buyer has certified that these additional scope and drawings are generalized and would not lead to any restrictive bidding.

Buyer Added Bid Specific Terms and Conditions

1. Generic

OPTION CLAUSE: The Purchaser reserves the right to increase or decrease the quantity to be ordered up to 25 percent of bid quantity at the time of placement of contract. The purchaser also reserves the right to increase the ordered quantity by up to 25% of the contracted quantity during the currency of the contract at the contracted rates. Bidders are bound to accept the orders accordingly.

2. Buyer Added Bid Specific ATC

Buyer uploaded ATC document [Click here to view the file.](#)

Disclaimer

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization. Buyer organization is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any eccentricity/restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and/or terms and conditions governing the bid. Any clause incorporated by the Buyer such as demanding Tender Sample, incorporating any clause against the MSME policy and Preference to make in India Policy, mandating any Brand names or Foreign Certification, changing the default time period for Acceptance of material or payment timeline governed by OM of Department of Expenditure shall be null and void and would not be considered part of bid. Further any reference of conditions published on any external site or reference to external documents/clauses shall also be null and void. If any seller has any objection/grievance against these additional clauses or

otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations. Also, GeM does not permit collection of Tender fee / Auction fee in case of Bids / Forward Auction as the case may be. Any stipulation by the Buyer seeking payment of Tender Fee / Auction fee through ATC clauses would be treated as null and void.

[This Bid is also governed by the General Terms and Conditions.](#)

In terms of GeM GTC clause 26 regarding Restrictions on procurement from a bidder of a country which shares a land border with India, any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. While participating in bid, Bidder has to undertake compliance of this and any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

---Thank You---



An Autonomous Scientific Society under Ministry of Electronics & Information Technology (MeitY),
Govt. of India

www.ernet.in

TENDER

For

SELECTION OF SYSTEM INTEGRATOR

For

**Supply and Setting up of ICT Infrastructure at Data Centres
and Remote Sites and Operation & Maintenance**

Table of Contents

Section I: Notice Inviting Tender (NIT)	8
Section II: Instructions to Bidders (ITB)	11
1. The Tender Document	12
1.1 Basic Tender Details.....	12
1.2 Interpretations, Definitions, Abbreviations	12
1.3 Overview of Contents.....	12
1.4 Sections of the Tender Document	12
1.5 Forms (To be filled, digitally signed, and uploaded by Bidders).....	13
1.6 Other Form & Formats	14
2 ERNET India - Rights and Disclaimers	14
2.1 ERNET India.....	14
2.2 Right to Intellectual Property:.....	14
2.3 Right to Reject any or all Bids.....	14
2.4 Disclaimers.....	15
3 Bidders - Eligibility and Preferential Policies	15
3.1 Bidders	15
3.2 Eligibility Criteria for Participation in this Tender.....	15
4 Purchase preference to Make in India	16
4.1 Definition of Local Content and Categories of Local Suppliers.....	16
4.2 Eligibility to participate	16
4.3 Classification of Procurement and purchase preference methodology:.....	16
4.4 Calculation of Local Content in bid to be taken care by bidder	17
4.5 Verification of local content and violations:.....	17
5 Bid Prices, Taxes and Duties	17
5.1 Prices	17
5.1.1 Competitive and Independent Prices.....	17
5.1.2 Price Schedule.....	18
5.2 Firm/ Variable Price.....	18

5.3	Goods and Services Tax (GST).....	18
5.4	Payments.....	19
6	Downloading the Tender Document; Corrigenda and Clarifications.....	19
6.1	Downloading the Tender Document.....	19
6.2	Corrigenda/ Addenda to Tender Document	19
6.3	Clarification on the Tender Document	20
7	Pre-bid Meeting	20
8	Preparation of Bids	20
8.1	The bid.....	20
8.2	Documents comprising the bid:	21
8.3	Bid Validity.....	22
8.4	Bid Security - Related Documents.....	22
8.5	Non-compliance with these provisions	23
9	Signing and Uploading of Bids	23
9.1	Relationship between Bidder and e Procurement Portal (GeM).....	23
9.2	Signing of bid	23
9.3	Submission/ uploading of Bids.....	24
10	Bid Opening	25
11	Evaluation of Bids and Award of Contract	25
11.1	General norms	25
11.2	Evaluation of Bids.....	26
11.3	Technical Evaluation	26
11.4	Evaluation of Financial Bids	27
12	Award of Contract.....	28
12.1	The ERNET India's Rights	28
12.2	Signing of Non-Disclosure Agreement.....	28
12.3	Purchase Order and Signing of Contract	28
13	Integrity Pact:	29
	Section III: General Conditions of Contract(GCC)	30
1.	General.....	31
1.1	Tenets of Interpretation.....	31

1.2	Definitions.....	31
1.3	Abbreviations:	34
2	The Contract	34
2.1	Language of Contract	35
2.2	The Entire Agreement.....	35
2.3	Severability	35
2.4	Parties.....	35
2.5	Contract Documents.....	35
3	Governing Laws and Jurisdiction	36
3.1	Governing Laws and Jurisdiction	36
4	Communications.....	36
4.1	Communications.....	37
4.2	The person signing the Communications	37
4.3	Address of the parties for sending communications by the other party.....	37
5	Contractor’s Obligations and restrictions on its Rights	37
5.1	Changes in Constitution/ financial stakes/ responsibilities of a Contract’s Business ...	38
5.2	Obligation to Maintain Eligibility and Qualifications.....	38
5.3	Consequences of a breach of Obligations	38
5.4	Assignment and Sub-contracting	38
5.5	Indemnities for breach of IPR Rights or from other issues.....	38
5.6	Confidentiality and IPR Rights	39
5.7	Performance Bond/ Security.....	40
5.8	Permits, Approvals and Licenses	41
6	Scope of work, Project Management and Technical Specifications.....	41
7	Inspection and Quality Assurance	46
7.1	Tests and Inspections.....	46
7.2	Consequence of Rejection	46
7.3	ERNET India’s right of Rejection of Inspected Equipment	47
8	Transfer of Assets and Insurance	47
8.1	Transfer of Assets.....	47
8.2	Insurance.....	47

9	Terms of Delivery and delays	48
9.1	Effective Date of Contract	48
9.2	Place (destination/Location) of Delivery	48
9.3	Terms of Delivery, Installation, testing, commissioning & Acceptance	48
9.4	Delay in the contractor’s performance	51
9.5	Extension of Delivery Period and Liquidated Damages:	51
9.6	Force Majeure:	52
10	Prices and Payments Terms:	52
11	Arbitration	54
12	Defaults, Breaches, Termination, and closure of Contract	55
12.1	Termination due to Breach, Default, and Insolvency	55
12.2	Termination for Default/ Convenience of ERNET India	56
12.3	Closure of Contract	57
	Section IV: Bill of Material	58
	Section V: Technical Specifications	69
	Section VI: Qualification Criteria	243
A.	Bidder’s Qualification Criteria	244
B.	Original Equipment Manufacturer (OEM)’s Criteria	246
	Section VII: Scope of Work	249
1.	Project Overview	250
2.	Overall Deliverables of Contractor	250
3.	Roles and Responsibilities of Contractor	251
4.	Role and Responsibilities of contractor at Data Center:	251
5.	Role and Responsibilities of contractor at Disaster Recovery Data Center (DR):	252
6.	Role and Responsibilities of contractor at Remote Sites & its Integration ...	253
7.	Role and Responsibilities of Contractor i.r.o EMS, DCIM and related software applications:	254
8.	Role and Responsibilities of Contractor i.r.o Integration of DC equipment(s) with Phase-1 IT equipment(s):	256
9.	General Activities to be performed by Contractor for the project: -	258

10. Acceptance Testing (AT)	259
11. Training	260
12. Scope of Work for Operation and Maintenance	260
12.1 Asset Management Services	262
12.2 Preventive Maintenance Services	263
12.3 Installation/configuration and reconfiguration/rollback of equipment ...	263
12.4 Network Management Services	263
12.5 Server Management Services	264
12.6 Enterprise Management (EMS) & Data Centre Infrastructure Management (DCIM) Services	265
12.7 Security Administration and Management Services	265
12.8 Disaster Recovery Configuration Services	266
12.9 Network Management Services including Security Incident Lifecycle Management	267
12.10 Remote site support	267
12.11 Vendor Management Services	267
12.12 Change management Services	268
12.13 Help Desk Support	268
12.14 Dash boarding and Reporting	269
Daily Reports	269
Weekly reports	269
Monthly reports.....	269
Quarterly reports	270
Half-Yearly reports.....	270
Incident Reporting	270
13. Manpower for Operation & Management at DC , DR and at Delhi	271
13.1 Minimum Manpower to be deployed for one year from the start of Operation and maintenance	272
13.2 Manpower Specification	273
13.3 Work profile of Manpower to be deployed	274
14. Project Handover Plan	277

Section VIII: Service Level Agreement during Operation & Maintenance.....	278
1 Service Level during Operation & Maintenance period for Equipment:.....	279
A. For Equipment at DC & DR procured via this bid:	279
B. For Equipment procured at DC via the Phase-1 bid(by CDAC):	279
C. For equipment at remote sites:	279
D. Help Desk support during O&M period for services:	280
E. Help Desk Support Services Level.....	280
F. Security and Incident Management Service Levels	282
G. Manpower Service Level Agreement:	283
BIDDING FORMS	284
Form 1: Bid Form (Covering Letter)	285
Form 1.1: Bidder Information	287
Form1.2: Eligibility Declarations	289
Form 2: Bill of Material - Compliance	291
Form3: Technical Specifications- Compliance	292
Form3A: Unpriced Make & Model Details- Compliance.....	293
Form4: Qualification Criteria - Compliance	298
Form5: Terms & Conditions- Compliance	299
Form 6: Check-List for Bidders.....	300
Form 7: Documents relating to Bid Security.	302
Form8: Integrity Pact	303
Form 9 : Make in India Certificate.....	307
Form 10: Non-Disclosure Agreement (To be submitted on Non-Judicial Stamp Paper of Rs 100/-)	308
Format 1.1: Bank Guarantee Format for Performance Security	313
Format 1.2: No Claim Certificate	315
Format 2: Authorization for Attending Pre-bid Conference.	316
Form 11 Financial Bid (BoQ).....	318
Financial Bid (BoQ) <i>(This duly filled sheet must be uploaded under "upload Financial Document" tab on GeM Portal.</i>	318

Section I: Notice Inviting Tender (NIT)

1. Notice Inviting Tender (hereinafter referred to as “NIT”)

ERNET India, an autonomous society of Ministry of Electronics and Information Technology, Govt. of India mandated to consult and deploy ICT solution utilising latest technologies for education and research institutions of country. ERNET India invites proposals (hereinafter referred as the ‘bid(s)’) for entering into a Contract for **“Selection of System Integrator for Supply and Setting up of ICT Infrastructure at Data Centres and Remote Sites and Operation & Maintenance”**. The Tender Document bearing No./ xxxx (hereinafter referred to as ‘the Tender Document’) gives further details with regard to the invitation.

Only Class-I or Class-II Local Supplier as defined in Letter no. P45021/2/2017-PP (BE-II) dated 16.09.2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, Government of India (GoI) or as amended from time to time and until the date of submission of the bids by the bidders are eligible to participate in this tender.

2. The Tender

- 2.1. Bidders must read the complete ‘Tender Document’. This NIT is an integral part of the Tender Document and serves a limited purpose of invitation, and does not purport to contain all relevant details for submission of bids. Bidders must go through the complete Tender Document for details before submission of their Bids.
- 2.2. Availability of the Tender Document: -The Tender Document shall be published on the Government E-Marketplace of Govt. of India (GeM Portal). It shall be available for download after the date and time of the start of availability till the deadline for availability as mentioned on GeM Portal.
- 2.3. **Clarifications:** - A Prospective Bidder requiring any clarification regarding the Tender Document may do so using GeM Portal and also send to below mail IDs. Also, please feel free to contact Sh. Sunil Mishra, Joint Director (Contact no. 011-22170979), ERNET India sunilmishra@ernet.in with copy marked to anirudh@ernet.in & govind.ranjan@ernet.in for any query related to tender. Clarification should asked be in below format in excel and PDF sheet:

Sl. No	Tender Page No.	Section/ Clause No.	Tender Clause	Bidder’s Clarification Sought

3. Eligibility Criteria for Participation in this Tender

Subject to provisions in the Tender Document, participation in this Tender Process is open to all bidders who fulfil the ‘Eligibility’ and ‘Qualification criteria. Bidder should meet the following eligibility criteria as on the date of bid submission and should continue to meet these till the award of the contract. Bidder shall be required to declare fulfilment of Eligibility Criteria in Form 1.2 (Eligibility Declarations).

1. The Bidder must: be a Company registered in India under the Indian Companies Act 1956/2013 (as amended) with their registered office in India for the last five years or more as on 31.07.2022.

2. The bidder must:
 - a. not be insolvent, in receivership, bankrupt or being wound up and not have its business activities suspended by Government.
 - b. Not stand declared ineligible/ blacklisted/ banned/ debarred by Government .
3. The prices quoted should be competitive and without adopting any unfair/ unethical/ anti-competitive means. No attempt should be made to induce any other bidder to submit or not to submit an offer for restricting competition.
4. The Bidder must also fulfil other additional eligibility condition(s), if any, as prescribed in Tender Document (including addendums; if issued).
5. Bidders shall go through F.No.6/18/2019 – PPD dated 23rd July 2020 issued by Department of Public Procurement, Ministry of Finance, Govt. of India and declaration with regard to the of same should be given in Form 1.2 (Eligibility Declaration).
<https://doe.gov.in/sites/default/files/OM%20dated%2023.07.2020.pdf>

4. Pre-bid Meeting:

Prospective Bidders or their authorized representative may attend the Pre-bid meeting for seeking clarification on Tender Document in online mode at the time, date, as mentioned on GeM Portal.

5. Submission of Bids:

- 1) Bids must be uploaded on GeM portal till the deadline for submission mentioned on GeM Portal. Bidder must comply with the conditions of the GeM Portal, including registration, compatible Digital Signature Certificate (DSC) etc. In the case of downloaded documents, Bidder must not make any changes to the contents of the documents while uploading, except for filling in the required information.
- 2) Bidder must submit the bid complete in all respect; in the absence of which bid may be rejected.

6. Bid Opening

Bids received shall be opened online at the specified date and time mentioned on GeM Portal.

7. Disclaimers and Rights of ERNET India

The issue of the Tender Document does not imply that the ERNET India is bound to select bid(s), and it reserves the right, without assigning any reason, to:

- a) reject any or all of the Bids, or
- b) cancel the tender process at any stage; or
- c) abandon the procurement of Equipment(s) and Services; or
- d) issue another tender for identical or similar Equipment(s) and Services

Signed by
Tender Inviting Authority (TIA), ERNET India

Section II: Instructions to Bidders (ITB)

1. The Tender Document

1.1 Basic Tender Details

The 'Tender Document' (hereinafter referred to as the 'the Tender Document') details the terms and conditions for entering into a contract with System Integrator for the execution of turnkey project (BoM & Scope of work detailed as per Section-IV & Section -VII respectively). Bidders must go through the entire Tender Document for further details.

1.2 Interpretations, Definitions, Abbreviations

General Conditions of Contract (GCC), detailed Tenets of interpretation (GCC-clause 1.1), Definitions (GCC-clause 1.2), and Abbreviations (GCC-clause 1.3) in **Section III**, which shall also apply to the rest of the Tender Document.

1.3 Overview of Contents

- 1) the Sections, Forms and Formats comprising this Tender Document are described in Instruction To Bidders (ITB)-clauses 1.4, 1.5 and 1.6 below. Any generic reference to Tender Document shall also imply a reference to any/ all the sections, Forms, Formats and the BoM or other files that comprise this Tender Document.
- 2) Bidder must submit the bid in the Forms/ Formats mentioned in ITB-clauses 1.5 and 1.6 below along with signed tender document along with its all corrigendum and addendums. Bidder must declare in his bid Form (Form 1) that it has read, understood, complied, and stands bound by all requirements.

1.4 Sections of the Tender Document

1.4.1 Sections of the Tender Document

the Tender Document contains the following sections, which are described in subsequent sub-clauses:

- 1) Section I: Notice Inviting Tender (NIT)
- 2) Section II: Instructions to Bidders (ITB)
- 3) Section III: General Conditions of Contract (GCC)
- 4) Section IV: Bill of Material (BoM)
- 5) Section V: Technical Specifications
- 6) Section VI: Qualification Criteria
- 7) Section VII: Complete Scope of Work
- 8) Section VIII: Service Level Agreement

1.4.2 Section I: Notice Inviting Tender (NIT)

Section I – Notice Inviting Tender (NIT) provides a synopsis of information relevant for a Bidder.

1.4.3 Section II: Instructions to Bidders (ITB)

Section II: “Instructions to Bidders” - ITB provides the relevant information as well as instructions to assist the prospective Bidders in preparation and submission of Bids. It also includes the mode and procedure adopted for receipt/ opening/ evaluation of Bids, and contract award.

1.4.4 Section III: General Conditions of Contract (GCC)

Section III – General Conditions of Contract (GCC) describe the conditions that shall govern the resulting contract. In case of any conflict, provisions of GCC shall prevail over those in ITB and in case of any conflict of this tender document from GeM GTC, provisions of this tender document shall prevail over those in GeM GTC

1.4.5 Section IV: Bill of Material

Section IV – Bill of Material (BoM) describes the Equipment and Services required; Quantities and Units; City of Delivery; Bidder must fillup ‘Form 2: ‘Bill of Material-Compliance’.

1.4.6 Section V – Technical Specifications

Section V – This Section lays down the technical specification of the Equipment and services required. Bidders must give Compliance for all the specifications in Form 3: Technical Specifications compliance along with Form 3A- Unpriced Make & Model of offered equipment(s).

1.4.7 Section VI: Qualification Criteria:

Section VI: Qualification Criteria lay down the Qualifying Criteria for a bid/ Bidder to be considered a responsive bid/ bidder for further evaluation. Bids/ bidders not meeting these Qualification criteria shall be rejected as nonresponsive. Bidders must fill up ‘Form 4: Confirmation from Qualification Criteria’. Bidders shall attach statements and documents to confirm conformity to Qualification Criteria.

1.4.8 Section VII: Scope of Work defined in this section.

1.4.9 Section VIII: Successful Bidder must adhere Service Level Agreement as defined in Section VIII

1.5 Forms (To be filled, digitally signed, and uploaded by Bidders)

Please refer to clause 1.4 above to relate the following forms to the corresponding Sections.

- 1) Form 1: Bid Form (To serve as a covering letter to both the Technical and Financial Bids)
 - a) Form 1.1: Bidder Information
 - b) Form 1.2: Eligibility Declarations
- 2) Form 2: Bill of Material - Compliance
- 3) Form 3: Technical Specifications- Compliance
 - (a) Form 3A: Unpriced Make and Model of Offered equipment(s)
- 4) Form 4: Qualification Criteria - Compliance
- 5) Form 5: Terms & Condition compliance
- 6) Form 6: Checklist for the Bidders
- 7) Form 7: Documents Relating to Bid Security

- 8) Form 8: Integrity Pact
- 9) Form 9: Make in India Certificate
- 10) Form 10: Non-Disclosure Agreement
- 11) Form 11: Financial bid (BOQ) Sheet (shall be uploaded under the tab of “**Upload Financial Document**” on GeM Portal).
- 12) Signed tender document along with its all Clarifications, corrigendum and addendums

1.6 Other Form & Formats

- 1 Format 1.1: Bank Guarantee Format for Performance Security
- 2 Format 1.2: No Claim Certificate
- 3 Format 2: Authorization for Attending Pre-bid Conference.

2 ERNET India - Rights and Disclaimers

2.1 ERNET India

ERNET India is the National Research and Education Network dedicated to support the needs of the research and education community within the country. It was established in 1998 as an autonomous scientific society registered under The Societies Registration Act, 1860 and works under the administrative control of Ministry of Electronics and Information Technology, Government of India. ERNET India operates terrestrial and satellite network and serving many institutions in various sectors, namely, health, agriculture, higher education, schools and science & technology.

Bids are to be addressed to the Registrar & CPO , ERNET India in the ERNET India. The Tender Inviting Authority or its representative is the designated officer for uploading and clarifying this Tender Document. The contract may designate, as required, Officer and Consignee(s) and paying authority who shall discharge designated function during contract execution.

2.2 Right to Intellectual Property:

The Tender Document and associated correspondence shall always remain the property of the ERNET India.

2.3 Right to Reject any or all Bids

The ERNET India reserves its right to accept or reject any or all Bids, abandon/ cancel the Tender process at any stage, and issue another tender for the same or similar Equipment at any time before the award of the contract. It would incur no liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for such action(s).

2.4 Disclaimers

2.4.1 Regarding Purpose of the Tender Document

The Tender Document is neither an agreement nor an offer to prospective Bidder(s) or any other party hereunder. The purpose of the Tender Document is to provide the Bidder(s) with information to assist them in participation in this Tender Process.

2.4.2 Regarding Documents/ guidelines

The Tender Document, ensuing communications, and Contracts shall determine the legal and commercial relationship between the bidders/ contractors and the ERNET India.

2.4.3 Regarding Information Provided

Information contained in the Tender Document or subsequently provided to the Bidder(s) is on the terms and conditions set out in the Tender Document or subject to which that was provided. Similar terms apply to any information provided in documentary or any other form, directly or indirectly, by the ERNET India or any of its authorised employees or its associated agencies in connection with this tender.

2.4.4 Regarding Tender Document:

- 1) The Tender Document does not purport to contain all the information Bidder(s) may require. It may not address the needs of all Bidders. They should conduct due diligence, investigation, and analysis, check the information's accuracy, reliability, and completeness, and obtain independent advice from appropriate sources. Information provided in the Tender Document to the Bidder(s) is on a wide range of matters, some of which may depend upon interpreting the law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The ERNET India, its employees and other associated agencies accept no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.
- 2) The ERNET India, its employees and other associated agencies make no representation or warranty for the accuracy, adequacy, correctness, completeness or reliability, assessment, assumption, statement, or information in the Tender Document. They have no legal liability, whether resulting from negligence or otherwise, for any loss, damages, cost, or expense that may arise from/ incurred/ suffered howsoever caused to any person, including any Bidder, on such account.

3 Bidders - Eligibility and Preferential Policies

3.1 Bidders

Subject to provisions in the following clauses in this section and provisions in Tender Document, this invitation for Bids is open to all bidders who fulfil the 'Eligibility Criteria' and 'Qualification Criteria' stipulated in the Tender Document.

3.2 Eligibility Criteria for Participation in this Tender

As defined in NIT. It is not being reproduced here for the sake of brevity.

4 Purchase preference to Make in India

Purchase preference to the qualified bidders for Make in India would be provided in line with Public Procurement (Preference to Make in India) Order 2017” (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised and amended from time to time including the Letter No. P-45021/2/2017-PP (BE-II). Dated 16th September, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI as amended from time to time and F. No. W-43/4/2019-IPHW-MeitY 07/09/2020 issued by IPHW division of MeitY.

4.1 Definition of Local Content and Categories of Local Suppliers

Bidders/Contractors are divided into three categories based on Local Content. Local content means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the Item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.

- a) 'Class-I local Supplier' is a supplier with local content equal to or more than 50%.
- b) 'Class-II local Supplier' is a supplier with local content equal to or more than 20%, but less than that applicable for Class-I local Supplier.
- c) 'Non - Local Supplier' is a supplier with local content less than that applicable for Class-II local Supplier, in sub-clause above.
- d) The margin of purchase preference shall be 20%.

4.2 Eligibility to participate

- a) Classes of Local Suppliers eligible to Participate: Based on the Make in India Policy, only Class-I and Class-II local Suppliers shall be eligible to participate in this bid.
- b) Minimum local content for eligibility to participate shall be 20%.
- c) **Non- local suppliers are not eligible to participate in this bid.**

4.3 Classification of Procurement and purchase preference methodology:

Under this tender, Procurement of Equipment(s) and services are not divisible in nature. This is an integrated work and objective of work is to setup equipment(s) at Data Center & at multiple remote locations. Remote Locations equipment(s) shall be connected with Data Center Equipment(s) over Internet/MPLS to transfer the data which requires the work to be carried out as turnkey project & in a comprehensive manner wherein contractor is responsible for design, supply, installation, configuration, commissioning, training and also operation and maintenance to ensure reliable functioning of envisaged project. As such work is clearly indivisible in nature and required to be carried out as a turnkey project consisting procurement and integration of networking, security and other hardware and software and thereafter operation and maintenance of installed equipment(s). Hence bids will be evaluated on total bid price and Class-I local supplier will get purchase preference over Class-II local supplier as per following procedure:

- a) Among all qualified bids, the lowest bid shall be termed as L-1. If L-1 is 'Class-I local Supplier', the contract shall be awarded to L-1.
- b) If L-1 is not 'Class-I local Supplier', the lowest bidder among the 'Class-I local Supplier' shall be invited to match the L-1 price subject to Class-I local Supplier's quoted price falling within the margin of purchase (20%) preference, and the contract shall be awarded to such 'Class-I local Supplier' subject to matching the L-1 price.

- c) If such lowest eligible 'Class-I local Supplier' fails to match the L-1 price, the 'Class-I local Supplier' with the next higher and so on, bid within the margin of purchase preference shall be invited to match the L-1 price, and the contract shall be awarded accordingly. If none of the 'Class-I local Supplier' within the margin of purchase (20%) preference matches the L-1 price, the contract will be awarded to the L-1 bidder.
- d) No purchase preference will be given to Class-II local suppliers.

4.4 Calculation of Local Content in bid to be taken care by bidder

As this bid requires supply of multiple items (say “X1”, “X2” and “X3”) by a single bidder, **the local content calculation by the bidder in the bid shall be done as per below mentioned formula & conditions as per available on DPIIT website.**

<https://dpiit.gov.in/sites/default/files/RTI%20FAQ.pdf>

- a) Local content = $((\text{Sale price of "X1"} - \text{Value of imported content in "X1"}) + (\text{Sale price of "X2"} - \text{Value of imported content in "X2"}) + (\text{Sale price of "X3"} - \text{Value of imported content in "X3"})) * 100 / (\text{Sale price of "X1"} + \text{Sale price of "X2"} + \text{Sale price of "X3"})$. Where, “Sale price” means price excluding net domestic indirect taxes and “Value of imported content” means price of imported content inclusive of all customs duties.
- b) The cost of transportation, insurance, installation, commissioning, training and after sales service support like AMC/CMC etc. will not be taken into account for calculating local content in any equipment.

4.5 Verification of local content and violations:

- 1) The 'Class-I local Supplier' / 'Class-II local Supplier' at the time of tender, bidding, or solicitation shall be required to indicate the percentage of local content and provide self-certification that the item offered meets the local content requirement for 'Class-I local Supplier' / 'Class-II local Supplier', as the case may be.
- 2) The 'Class-I local Supplier' / 'Class-II local Supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) giving the percentage of local content as specified in Form-9.
- 3) ERNET India reserves the right to seek any clarification/document/certification w.r.t compliance with MII orders referred above till the time of completion of tender process.
- 4) False declarations will be in breach of the code of integrity under rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

5 Bid Prices, Taxes and Duties

5.1 Prices

5.1.1 Competitive and Independent Prices

- a) The prices should be arrived at independently, without restricting competition, any consultation, communication, or agreement with any other bidder or competitor relating to:

- i) those prices; or
 - ii) the intention to submit an offer; or
 - iii) the methods or factors used to calculate the prices offered.
- b) The prices should not be knowingly disclosed by the Bidder, directly or indirectly, to any other bidder or competitor before bid opening or contract award unless otherwise required by law.

5.1.2 Price Schedule

- 1) Bidders are to quote value of each line item in the Financial Bid (BoQ) which is to be uploaded on GeM Portal. Based on the scope of work specified in Section-VII, if the bidder(s) feel it necessary to quote any other item other than the item specified in Bill of Material then it may quote the same in the financial (BoQ) under '**Any other item**' and also provide the specification of same along with technical bid. In case of any discrepancy between rates mentioned in figures and words, the later shall prevail. In case of any arithmetic mistake committed by bidder in Financial bid (BoQ) then ERNET India reserve the right to correct the same by taking unit price quoted by the bidder and quantities specified by the ERNET India.
- 2) Bidders shall fill in their rates other than zero value. Bid will be liable to be rejected if bidder **has filled Rs. 0 (zero) for any line item** except for the line item wherein mentioning of zero value is allowed in Financial Bid (BoQ).
- 3) The quoted unit price shall be considered to include all relevant financial implications.

5.1.3 Currencies of Bid and Payment

The currency of bid and payment shall only be Indian Rupees. All payments shall also be made in Indian Rupees only.

5.1.4 Non-compliance

Bids, wherein prices are quoted in way other than the specified format, may be rejected as non-responsive.

5.2 Firm/ Variable Price

5.2.1 Firm Price

Prices quoted by Bidder shall remain firm and fixed during the currency of the contract and not subject to variation on higher side any account.

5.3 Goods and Services Tax (GST)

- 1) Bidders should ensure that they are GST compliant Bidder should be registered under GST and furnish GSTIN number and GST Registration Certificate in their bids.
- 2) Bidder/Contractor undertakes that in case of non-compliance by the Bidder(s) of the GST provisions which results in blockage/reversal of any input tax credit to ERNET

India, Bidder/Contractor shall be liable to indemnify the ERNET India any such loss of input credit including interest, penalty and all incidental expenses incurred by ERNET India. Such indemnification may also be by way of invocation of any security deposit, deduction from any payment that ERNET India has to make to the Bidder/Contractor, as per the discretion of the ERNET India.

- 3) Bidder/Contractor undertakes to raise invoice within 10 days from date when the right to raise invoice and demand for payment accrues as per the contract terms. In case invoice is raised and submitted before the due date; then ERNET India reserves the right to return such invoice(s) to the Bidder/Contractor. In such a situation Bidder/Contractor would be required to raise fresh invoice as per the contract terms.
- 4) If the Bidder/Contractor fails to adhere the terms & conditions of the contract and ERNET deducts Liquidated Damages and/or SLA penalties for the same, then in such a case; ERNET India will charge GST over and above the Liquidated Damages and/or SLA penalties; as the case may be; and same shall be recovered from the Bidder/Contractor. This may vary; depending on the prevailing rules on the subject when such deduction is made.
- 5) Along with the invoice; Bidder/Contractor would be required to submit relevant documentary evidence to the effect that invoice submitted was issued either through e-Invoice system of GST or has been updated on GSTN portal using Invoice Furnishing Facility (IFF).
- 6) In case, in future any GST liability is required to be borne by ERNET India; which was the responsibility of the Bidder/Contractor, then the same shall be claimed from the Bidder/Contractor by way of raising debit notes.
- 7) ERNET India reserves the right to ask the Bidder/Contractor to submit relevant documents to ensure that they are GST compliant and in such a case Bidder/Contractor shall forthwith provide all such documents as may be required by ERNET India.

5.4 Payments

5.4.1 General

Payment terms laid down in clause GCC 10 shall be applicable.

6 Downloading the Tender Document; Corrigenda and Clarifications

6.1 Downloading the Tender Document

The Tender Document shall be published and be available for download as mentioned on GeM portal. The Bidders can obtain the Tender Document after the date and time of the start of availability till the deadline for availability.

6.2 Corrigenda/ Addenda to Tender Document

Before the deadline for submitting bids, the ERNET India may update, amend, modify, or supplement the information, assessment or assumptions contained in the Tender Document by issuing Clarifications, corrigenda and addenda. The Clarification, corrigenda

and addenda shall be published in the same manner as the original Tender Document published on GeM portal. Its bidders(s) responsibility to check the GeM Portal for any Clarification/corrigenda/ addenda. Any Clarification or corrigendum or addendum thus issued shall be considered a part of the Tender Document.

6.3 Clarification on the Tender Document

A Bidder may seek clarification of the Tender Document through GeM Portal, provided the clarifications are submitted atleast one day before the pre-bid meeting . The response to the clarifications (If any) shall be shared on the GeM portal as well as on ERNET India's website. Any modification of the Tender Document that may become necessary in view of response given to the clarification; shall be made by the ERNET India by issuing an Addendum/ Corrigendum as per the sub-clause 6.2 above.

7 Pre-bid Meeting

- 1) Prospective bidders interested in participating in this tender may attend **online** Pre-bid meeting to seek clarification to the Tender Document. Due date and time of pre-Bid will be informed on GeM Portal.
- 2) Participation is not mandatory. However, if a bidder chooses not to (or fails to) participate in the Pre-bid meeting and/or does not submit a written query via emails, as specified in NIT, it shall be assumed that they have participated in this tender process only after understanding the tender document in its entirety.
- 3) The pre-bid meeting will be held online mode. Maximum of two People from an organisation will be allowed to attend the Pre-bid meeting. Delegates participating in the Pre-bid meeting must sent an email from its organisation email account with detail of person who will be attending the pre-bid meeting.
- 4) After the Pre-bid meeting, clarifications (if required) shall be published on the ERNET India's website and on GeM portal. If required, a corrigendum to the Tender Document shall be issued, containing amendments to the provision(s) of the Tender Document, which shall form integral part of the Tender Document. To give reasonable time to the prospective bidders to take such clarifications into account in preparing their bids, the ERNET India may suitably extend, as necessary, the deadline for the bid submission.

8 Preparation of Bids

8.1 The bid

8.1.1 Language of the bid

The bid submitted by Bidder and all subsequent correspondence and documents relating to the bid exchanged between Bidder and the ERNET India shall be written in English. However, the language of any printed literature furnished by Bidder in connection with its bid may be written in any other language provided a translation accompanies the same in the bid language. For purposes of interpretation of the bid, translation in the language of the bid shall prevail.

8.1.2 Local Conditions and Factors

Bidders shall themselves be responsible for compliance with Rules, Regulations, Laws and Acts in force from time to time at relevant places. On such matters, the ERNET India shall have no responsibility and shall not entertain any request from the bidders in these regards.

8.1.3 Cost of Bidding

The Bidder(s) shall bear all direct or consequential costs, losses and expenditure associated with or relating to the preparation, submission, and subsequent processing of their Bids, including but not limited to preparation, copying, postage, uploading, downloading, delivery fees, expenses associated with any submission of samples, demonstrations, or presentations which the ERNET India may require, or any other costs incurred in connection with or relating to their Bids. All such costs, losses and expenses shall remain with the Bidder(s), and the ERNET India shall not be liable in any manner whatsoever for the same or any other costs, losses and expenses incurred by a Bidder(s) for participation in the Tender Process, regardless of the conduct or outcome of the Tender Process.

8.1.4 Interpretation of Provisions of the Tender Document

The provisions in the Tender Document must be interpreted in the context in which these appear. Any interpretation of these provisions far remote from such context or other contrived or in between-the-lines interpretation is unacceptable.

8.1.5 Alternative Bids not allowed

Conditional offers, alternative offers, multiple bids by a bidder shall not be considered. The GeM Portal shall permit only one bid to be uploaded.

8.2 Documents comprising the bid:

8.2.1 Technical bid

"Technical Bid" shall include inter-alia the original or scanned copies of duly inked signed or digitally signed copies of the following documents in .pdf format. .Pdf documents should not be password protected. **No price details should be given or hinted in the Technical bid:**

- 1) Form 1: bid Form (to serve as covering letter and declarations applicable for both the Technical bid and Financial bid);
 - a) Form 1.1: Bidder Information;
 - b) Form 1.2: Eligibility Declarations;
- 2) Form 2: Bill of Material (BoM) - Compliance: Bidders should fill this form to detail the Schedules of Equipment & Services offered by them, maintaining the same numbering and structure. Bidder shall also provide compliance statement of Schedule-IV as per attached Form 2.
- 3) Form 3 - Technical Specifications- Compliance: Bidder shall upload the required and relevant documents like make & model, technical data, literature, drawings, datasheets, test Reports/ Certificates and or/ or Type Test Certificates (if applicable/ necessary) with supporting documents, to establish that the Equipment and Services

offered in the bid fully conform to the Equipment and Services specified by the ERNET India in the Tender Document. Bidder shall also provide compliance statement of Schedule-V as per attached Form 3 along with filled Form 3.1

- 4) Form 4: 'Qualification Criteria- Compliance': Documentary evidence needed to establish the Bidder's and OEMs qualifications and MAF as stipulated in Section VI: Qualification Criteria as follows. Besides the stipulated documents, other supporting documents, literature, pamphlets may also be attached.
- 5) Form 5 – Terms & Condition Compliance: Bidder must submit compliance of Terms & conditions as per Form-5.
- 6) Form 6- Checklist for the Bidders. Bidder must also upload the Checklist given in the Tender Document as Form 6 to confirm that it has complied with all the instructions in the Tender Document, and nothing is inadvertently left out. This checklist is only for general guidance and is not comprehensive, and does not absolve Bidder from complying with all the requirements stipulated elsewhere in the Tender Document.
- 7) Form 7: Documents relating to Bid Security: A Bid Securing Declaration (BSD) in lieu of bid security in the format provided therein shall be uploaded as per ITB clause 8.4.
- 8) Form 8: Integrity Pact.
- 9) Form 9: Make in India Certificate [To be certified by statutory auditor or cost auditor of the company (in the case of companies) giving the percentage of local content].
- 10) Any other format/ form if stipulated or if considered relevant by the bidder

8.2.2 Financial bid

Form-11 : "Financial bid " shall comprise the Price Schedule considering all financially relevant details, including Taxes and Duties as per as per Financial Bid (BoQ) Proforma . This duly filled sheet must be uploaded under "**upload Financial Document**" tab on GeM Portal .

8.3 Bid Validity

- 1) Bid Validity should be equal to the period mentioned in Bid Document on GeM Portal. Any bid valid for a shorter period shall be rejected as nonresponsive.
- 2) If required, before the expiry of the original time limit, the ERNET India may request the bidders to extend the validity period for a specified additional period. The request and the bidders' responses shall be made in writing or electronically or as per GeM portal. A bidder who has agreed to the ERNET India's request for extension of bid validity, in no case, bidder shall be permitted to modify his bid.

8.4 Bid Security - Related Documents

- 1) All Bidders shall furnish/ upload a Bid Securing Declaration (BSD) as Form 7: Documents Relating to Bid Security, along with its Technical bid. The BSD is required to protect the ERNET India against the risk of the Bidder's unwarranted conduct as amplified under the sub-clause below.
- 2) The BSD provides for automatic suspension of the Bidder from being eligible for bidding in any tender in ERNET India for 2 years from the date of such enforcement.

This declaration shall stand enforced if Bidder breaches the following obligation(s) under the tender conditions:

- (a) withdraws or amends his bid or impairs or derogates from the bid in any respect within the period of validity of its bid; or
- (b) after having been notified within the period of bid validity of the acceptance of his bid by the ERNET India:
 - refuses to or fails to submit the original documents for scrutiny and/or the required Performance Security within the stipulated time as per the conditions of the Tender Document.
- 3) Unsuccessful Bidders' bid-Securing Declaration shall expire, if the contract is not awarded to them, upon:
 - (a) receipt by Bidder of the ERNET India's notification of cancellation of the entire tender process or rejection of all bids or
 - (b) declaration of the name of the successful bidder or
 - (c) forty-five days after the expiration of the bid validity (including any extension thereof)
- 4) The bid-Securing Declaration of the successful bidder shall stand expired only when Bidder has furnished the required Performance Security.

8.5 Non-compliance with these provisions

Bids are liable to be rejected as nonresponsive if a Bidder:

- 1) fails to provide and/ or comply with the required information, instructions etc., incorporated in the Tender Document or gives evasive information/ reply against any such stipulations.
- 2) furnishes wrong and/ or misleading data, statement(s) etc. In such a situation, besides rejection of the bid as nonresponsive, ERNET India will enforce Bid Security Declaration in such cases.

9 Signing and Uploading of Bids

9.1 Relationship between Bidder and e Procurement Portal (GeM)

The ERNET India is neither a party nor a principal in the relationship between Bidder and the organisation hosting the e-procurement portal (hereinafter called the GeM Portal). Bidders must acquaint and train themselves with the rules, regulations, procedures, and implied conditions/ agreements of the GeM Portal. Bidders intending to participate in the bid shall be required to register in the GeM Portal. Bidders shall settle clarifications and disputes, if any, regarding the GeM Portal directly with them.

9.2 Signing of bid

The individual signing/ digitally signing the bid or any other connected documents should submit Copy of Board Resolution and/ or Power of attorney on Stamp Paper for authorize signatory, which authorizes the signatory to commit and submit bids on behalf of the bidder in Form 1.1: Bidder Information. In case the bidder is awarded the contract then the person authorize by the bidder shall continue to act as the authorize representative

of the bidder till the time of completion of contract. Any change in authorize signatory should be informed forthwith to ERNET India along with the relevant document of authorize signatory.

9.3 Submission/ uploading of Bids.

9.3.1 Submission/ Uploading to the Portal

- 1) No manual Bids shall be made available or accepted for submission. In the case of downloaded documents, Bidder must not make any changes to the contents of the documents while uploading, except for filling the required information – otherwise, the bid shall be rejected as nonresponsive.
- 2) Bids shall be received only through GeM portal on or before the deadline for the bid submission.
- 3) Only one copy of the bid can be uploaded, and Bidder shall digitally sign all statements, documents, certificates uploaded by him, owning sole and complete responsibility for their correctness/ authenticity as per the provisions of the IT Act 2000as amended from time to time.
- 4) Bidders need to sign or up-load the Tender Document along with its clarifications, corrigendum & amendments. It is assumed that Bidder commits itself to comply with all the Sections and documents uploaded by the Tender Inviting Officer.
- 5) Bidder must upload scanned copies of originals (or self-attested copies of originals – as specified). Uploaded .Pdf documents should not be password protected. Bidder should ensure the clarity/ legibility of the scanned documents uploaded by them.
- 6) The ERNET India reserves its right to call for verification originals of all such self-certified documents from the Bidders at any stage of evaluation, especially from the successful Bidder(s) before the issue of Contract.
- 7) **Bidder shall upload the price as per Financial Bid (BoQ) on GeM Portal without any Zero values for any line item** except for the line item wherein mentioning of zero value is allowed in Financial Bid (BoQ).
- 8) The date and time of the deadline for the bid submission shall remain unaltered even if the specified date is declared a holiday for the Tender Inviting Officer.
- 9) The ERNET India shall not be responsible for any failure, malfunction or breakdown of the electronic system/internet issues used during the e-Tender Process at bidder's end.
- 10) The ERNET India may extend the deadline for bids submission in which case all rights and obligations of the ERNET India and the bidders previously subject to the original deadline shall then be subject to the new deadline for the bid submission.
- 11) Bid submitted through modalities other than those stipulated in tender document shall be liable to be rejected as nonresponsive.

9.3.2 Implied acceptance of procedures by Bidders

Submission of bid in response to the Tender Document is deemed to be acceptance of the tender procedures and terms & conditions of the Tender Document.

9.3.3 Withdrawal of Bids

- 1) The bidder may withdraw his bid before the bid submission deadline.
- 2) No bid should be withdrawn after the deadline for the bid submission and before the expiry of the bid validity period. If a Bidder withdraws the bid during this period, the ERNET India shall be within its right to enforce Bid Securing Declaration in addition to other punitive actions provided in the Tender Document for such misdemeanour.

10 Bid Opening

The date & time of the opening of bid is as stipulated in on GeM Portal.

11 Evaluation of Bids and Award of Contract

11.1 General norms

11.1.1 Evaluation based only on declared criteria.

The evaluation shall be based upon scrutiny and examination of all relevant data and details submitted by Bidder in its bid and other allied information deemed appropriate by ERNET India. Evaluation of bids shall be based only on the criteria/ conditions included in the Tender Document.

11.1.2 Minor Infirmary

- 1) In case of any minor infirmity in the bid document of bidder, the decision of the ERNET India shall be final in this regard.
- 2) Wherever necessary; the ERNET India shall convey its observation to Bidder through GeM portal asking Bidder to respond by a specified date. If Bidder does not reply by the specified date or gives an evasive reply without clarifying the point at issue in clear terms, that bid shall be liable to be rejected as non-responsive.

11.1.3 Clarification of Bids and shortfall documents

- 1) During the evaluation of Technical or Financial Bids, the ERNET India may, at its discretion, but without any obligation to do so, ask Bidder to clarify its bid within 3 days. The request for clarification shall be submitted on GeM Portal, and no change in prices or substance of the bid shall be sought, offered, or permitted that may grant any undue advantage to such bidder.
- 2) ERNET India may ask original documents of uploaded scanned copies. If any substantive discrepancy found between original and Scanned uploaded copies; then the bid shall be liable to be rejected as non-responsive. ERNET India may enforce Bid Security declaration in such cases.
- 3) The ERNET India reserves the right to seek any Clarification/information/ documents from the bidder. The requisite documents from any bidders may be taken as per GeM procedure after the technical bid opening. Decision in this regard shall be final and binding on all the bidders.

11.1.4 Contacting ERNET India during the evaluation

From the time of bid submission to awarding the contract, no Bidder shall contact the ERNET India on any matter relating to the submitted bid. If a Bidder needs to contact the ERNET India for any reason relating to this tender and/ or its bid, it should do so only in writing or electronically. Any effort by a Bidder to influence the ERNET India during the processing of bids, evaluation, bid comparison or award decisions shall be construed as a violation and bid shall be liable to be rejected as nonresponsive in addition to enforcement of Bid Security declaration.

11.2 Evaluation of Bids

11.2.1 The evaluation process:

This Tender Process comprises of two Bid system i.e Technical and Financial Bids. Initially, only the technical bids shall be opened on the stipulated date of opening of bids. After that, the technical bids evaluation shall be done to ascertain whether and how many bids are meeting the eligibility, qualification criteria and technical aspects. Opening of financial bids and their evaluation will be done in respect of only those bids which were submitted by those Bidders whose technical bid are declared successful after the evaluation process.

11.3 Technical Evaluation

Only substantively responsive bids shall be evaluated for technical evaluation. While evaluating the technical bid, conformity to the eligibility and qualification criteria, technical specifications of the offered Equipment and Services in comparison to those specified in the Tender Document will be ascertained. Additional factors incorporated in the Tender Document shall also be considered in the manner indicated there-in. Bids with deviations leading to non-confirmity shall be rejected as non-responsive. However, ERNET India reserves its right to consider and allow minor deviations in technical Conditions as per ITB-clause 11.1.2.

11.3.1 Evaluation of eligibility

ERNET India shall determine, to its satisfaction, whether the Bidders are eligible as per NIT-clause 3 above to participate in the Tender Process as per submission in Form 1.2: Eligibility Declarations in Form 1: bid Form. Bids that do not meet the required eligibility criteria prescribed shall be rejected as nonresponsive.

11.3.2 Evaluation of Qualification Criteria

Thereafter, ERNET India shall determine, to its satisfaction, whether the eligible bidders are qualified and capable in all respects to perform the Contract satisfactorily as per submission in Form 4. This determination shall, inter-alia, consider the Bidder's financial, technical or other prescribed eligibility for meeting requirements incorporated in the Tender Document.

11.3.3 Evaluation of Conformity to Bill of Material and Technical Specifications and other parameters specified in Tender document

Technical Evaluation Committee (TEC) will finally shortlist Technical Bids on the basis of technical solution, conformity of technical specifications, parameters, features offered vis- à-vis tendered specifications requirements, etc. If required, the short listed bidders may be asked for a detailed technical presentation, discussion on the solution and items offered in the bid. Further, TEC may ask the bidder to bring any selected Equipment(s)/items, sub items of their quoted equipment(s) for technical evaluation at ERNET India or any other location decided by TEC in specified time limit with three days. In case, bidder fails to bring their quoted equipment(s) within the stipulated time, for whatever reasons, their bid will not be considered for further evaluation. It is bidder's responsibility to showcase the desired parameter quoted in the bid by bidder. To do this, if bidder has to bring different tools, it will be responsibility of bidder to arrange at no cost to ERNET India.

11.3.4 Declaration of Technically Suitable Bidders and Opening of Financial Bids

Bids that succeed in the above technical evaluation shall be considered for financial evaluation. The list of such technically successful bidders and the date and time for the opening of their financial bids shall be declared on the GeM Portal.

11.4 Evaluation of Financial Bids

11.4.1 Financial Bids

- 1) Evaluation of the financial bids shall be on the price criteria only. Financial Bids of all Technically qualified bidders will be evaluated and an e-Reverse Auction (e-RA) process which will be conducted on GeM portal to determine the lowest cost (L-1) bidder.
- 2) The Reverse Auction (e-RA) process will be governed as per GeM Portal's procedures.
 - a. Bidder will be eliminated from participation in e-RA as per process defined in GeM Bid Document based on Grand Total Value quoted by the bidder on Gem Portal.
 - b. Price quoted on GeM Portal and Grand Total Value (GTV) of Financial Document uploaded in Pdf format on GeM portal should match. In case of any mismatch, ERNET India reserve the right to disqualify the bidder for further process and invoke the Bid security submitted in the form of Bid Security declaration.
- 3) In line with the policies of the Government of India, as amended from time to time, the ERNET India reserves the right to give purchase preferences to eligible categories of Bidders as indicated in the Tender Document.
- 4) Bidder must submit Price Break up {(Financial Bid(BoQ))} sheet during e-RA {(Financial Bid(BoQ))} if allowed on GeM.

11.4.2 Price Negotiation

ERNET India reserves its right to negotiate with the lowest acceptable bidder (L-1) after e Reverse Auction (e-RA) process, who is declared techno-commercially successful.

12 Award of Contract

12.1 The ERNET India's Rights

12.1.1 Right to Vary Quantities

ERNET India reserves the right to increase or decrease the quantity to be ordered up to 25 percent of final bid value at the time of placement of contract. The ERNET India also reserves the right to increase the ordered quantity by up to 25% of the final bid value during the contract period at the contracted rates. Bidders are bound to accept the orders accordingly.

12.2 Signing of Non-Disclosure Agreement

- 1) Those Bidders who are interested in getting Phase-1 equipment details and Data Center Layout will be required to sign (by its authorised signatory) and submit a Non-Disclosure Agreement(NDA) as per Form-10 before submission of bid and provide relevant documents with regard to meeting of the Annual average turnover Criteria as specified in Clause no. A (3) of Section VI .
- 2) The successful bidder/contractor shall sign a Non-Disclosure Agreement(NDA) with ERNET India as per Form-10 and submit the same within 14 days from the date of issue of contract.
- 3) The successful bidder shall also sign a Non-Disclosure Agreement with employees who are deployed in this project during implementation and operations.
- 4) The successful bidder/Contractor shall ensure that all persons, employees, workers and other individuals engaged by Bidder in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by the Bidder unless such person is found to be suitable in such verification and contractor shall retain the records of such verification and shall produce the same to ERNET India/CERT-IN as when requested. ERNET India/CERT-IN may also, if required, go for verification of manpower of contractor engaged for this project from government agencies.

12.3 Purchase Order and Signing of Contract

12.3.1 Selection of Successful Bidder(s)

The ERNET India shall award the contract to the Bidder whose bid is Technically successful and L-1 bidder (after e-RA process) if its final price (after negotiation if negotiation(s) are done found to be reasonable, as per evaluation criteria detailed in the Tender Document.

12.3.2 Performance Security

Within fourteen (14) days of issuance of contract through GeM Portal, performance Security as per details in GCC-5.8 shall be submitted by the successful bidder to the ERNET India and if it fails to do so within the specified period, it shall be lawful for the ERNET India at its discretion to annul the award and enforce Bid Securing Declaration.

12.3.3 Publication of Tender Result

The name and address of the successful Bidder(s) receiving the contract(s) shall be published in the GeM Portal and website of the ERNET India.

13 Integrity Pact:

The bidder must comply with the Integrity Pact (IP) as a preliminary qualification and sign the Integrity Pact (IP) as at Form 8 on plain paper.

Section III: General Conditions of Contract(GCC)

1. General

1.1 Tenets of Interpretation

Unless where the context requires otherwise, throughout the contract:

- 1) The heading of these conditions shall not affect the interpretation or construction thereof.
- 2) Writing or written includes matter either whole or in part, in digital communications, manuscript, typewritten, lithographed, cyclostyled, photographed, or printed under or over signature or seal or digitally acceptable authentication, as the case may be.
- 3) Words in the singular include the plural and vice-versa.
- 4) Words importing the masculine gender shall be taken to include other genders, and words importing persons shall include any company or association or body of individuals, whether incorporated or not.
- 5) Terms and expression not herein defined shall have the meanings assigned to them in the contract Act, 1872 (as amended) or the Sale of Goods Act, 1930 (as amended) or the General Clauses Act, 1897 (as amended) or of INCOTERMS, (current edition published by the International Chamber of Commerce, Paris) as the case may be.
- 6) Any reference to 'Equipment' shall be deemed to include the complete work i.e delivery, installation, testing, training, commissioning, warranty & any other service stipulated in tender document.
- 7) Any reference to 'Contract' shall be deemed to include all other documents as described in GCC-clause 2.5.
- 8) Any reference to any Act, Government Policies or orders shall be deemed to include all amendments to such instruments, from time to time.

1.2 Definitions

In the contract, unless the context otherwise requires:

- 1) "bid" (including the term 'tender', 'offer', 'quotation' or 'proposal' in specific contexts) means an offer to supply Equipment, services or execution of works made as per the terms and conditions set out in a document inviting such offers.
- 2) "Bidder" (including the term 'Bidder', 'contractor', 'System Integrator', or 'service provider' in specific contexts) means any person or firm or company, every artificial juridical person not falling in any of the descriptions of bidders stated herein before, including any agency branch or office controlled by such person, participating in a Tender Process.
- 3) "Bill of Quantities" {(including the term Financial Bid(BOQ)} means the financial sheet and complete Bill of Quantities forming part of the bid.
- 4) "Commercial Bank" means a bank, defined as a scheduled bank under section 2(e) of the Reserve Bank of India Act, 1934.

- 5) "Consignee" means the person to whom the Equipment are required to be delivered as stipulated in the contract or intimates at later date.
- 6) "Contract" means and includes 'Contract issued from GeM Portal', 'Purchase Order' or 'Supply Order' or 'Withdrawal Order' or 'Work Order' or , or 'Agreement' or a 'repeat order' accepted/ acted upon by the contractor or any amendment thereof, or a 'formal agreement', under specific contexts;
- 7) "Bidder/ Contractor/ Successful Bidder" (including the terms 'Supplier' or 'Service Provider', 'System Integrator', or 'Firm' or 'Vendor' or 'Bidder' under specific contexts) means the person, firm, company, with whom the contract is entered into and shall be deemed to include the contractor's successors (which is/are approved by the ERNET India), representatives, heirs, executors, and administrators as the case may be unless excluded by the terms of the contract.;
- 8) "Day", "Month", "Year" shall mean calendar day/ month or year (unless reference to financial year is clear from the context).
- 9) "General Conditions" means the General Conditions of Contract, also referred to as GCC.
- 10) "Government" means the Central Government or a State Government as the case may be and includes Autonomous Bodies, agencies and Public Sector Enterprises under it, in specific contexts;
- 11) "CERT-In" means Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology Government of India who has entrusted ERNET India for procurement of Equipment(s) and services laid down in this tender document. CERT-In is end user of this project.
- 12) "Inspection" means activities such as measuring, examining, testing, analysing, gauging one or more characteristics of the Equipment or services or works, and comparing the same with the specified requirement to determine conformity.
- 13) "Intellectual Property Rights" (IPR) means the rights of the intellectual property owner concerning a tangible or intangible possession/ exploitation of such property by others. It includes rights to Patents, Copyrights, Trademarks, Industrial Designs, Geographical indications (GI).
- 14) "Parties": The parties to the contract are the "Bidder/successful bidder/Contractor" as defined in this clause (7) above and the ERNET India;
- 15) "Performance Security" (includes the terms 'Security Deposit' or 'Performance Bond' or 'Performance Bank Guarantee' or other specified financial instruments in specific contexts) means a monetary guarantee to be furnished by the successful Bidder or Contractor in the form prescribed for the due performance of the contract;
- 16) "Location of Delivery" the delivery of the Equipment shall be deemed to take place on delivery of the Equipment, at following places (as defined in BoM- Section-IV) as per the terms and conditions of the contract.
- 17) "Consignee" The consignee at his premises; or the consignee at the destination station in case of a contract stipulating for delivery of Equipment at the destination station.

- 18) "Procurement" (or 'Purchase', or 'Government Procurement/ Purchase') means the acquisition of Equipment/ Services/ works by way of purchase, either using public funds or any other source of funds (e.g. grant etc.), by ERNET India, The term "procure"/ "procured" or "purchase"/ "purchased" shall be construed accordingly;
- 19) "The Procuring Entity/Organisation" means ERNET India in its capacity as Implementing agency of CERT-In procuring Equipment & Services;
- 20) "Procurement Officer" means the officer dealing the project issuing the Tender Document, Purchase order from GeM and/or the signing contract or etc. on behalf of the ERNET India;
- 21) "Specification" or "Technical Specification" means the drawing/ document/ standard or any other details governing the supply of Equipment or performance of services that prescribes the requirement to which Equipment or services have to conform as per the contract.
- 22) "Signed" means ink signed or digitally signed with a valid Digital Signature as per IT Act 2000 (as amended from time to time).
- 23) "Tender"; "Tender Document"; "Tender Enquiry" or "Tender Process": 'Tender Process' is the whole process from the publishing of the Tender Document till the resultant award of the contract. 'Tender Document' means the document (including all its sections, forms, formats, etc.) published by the ERNET India on GeM Portal to invite bids in a Tender Process. The Tender Document and Tender Process may be generically referred to as "Tender" or "Tender Enquiry", which would be clear from context without ambiguity.
- 24) "Tender No./ xxxx" refers to the GeM Bid Number, Bidders should add this number same as GeM Bid Number in all documentation pertaining to this tender.
- 25) "GeM Portal"; (includes e procurement) Government e Marketplace website on which this tender will be hosted and other tender related activities will be performed.
- 26) "Central Sites/ Central Location"; Two Data Centres proposed in this bid, one will be used as Primary Data Center (DC) and another will be as Disaster recovery Data Center (DR).
- 27) "Remote Sites"; Locations where equipment(s) will be delivered and will be connected to Central sites through IPSec over MPLS VPN.

1.3 Abbreviations:

Abbreviation	Definition
BOQ	Bill of Quantities (Financial Bid)
BSD	Bid Securing Declaration
DC	Primary/ Main Data Center
DR	Disaster Recovery Data Center
DP	Delivery Period
DPIIT	Department for Promotion of Industry and Internal Trade
DSC	Digital Signature Certificate
e-RA	Electronic Reverse Auction
EFT/ NEFT	(National) Electronic Funds Transfer
GCC	General Conditions of Contract
GeM	Government e-Marketplace
GeM ATC	GeM Additional Terms and Condition
GeM GTC	GeM General Terms and Conditions
GeM STC	GeM Standard Terms and Conditions
GST	Equipment and Services Tax
IEM	Independent External Monitor
IPR	Intellectual Property Rights
INR	Indian Rupee
ITB	Instructions To Bidders
MII	Make in India
MPLS	Multi-Protocol Label Switching
NIT	Notice Inviting Tender
OEM	Original Equipment Manufacturer
PAN	Permanent Account Number
P.O	Purchase Order
RCM	Reverse Charge Mechanism
TDS	Tax Deducted at Source
TIA	Tender Inviting Authority

2 The Contract

2.1 Language of Contract

The contract shall be written in the Official Language or English. All correspondence and other contract documents, which the parties exchange, shall also be written/ translated accordingly in that language. For purposes of interpretation of the contract, the English documents/ translation shall prevail.

2.2 The Entire Agreement

The Contract to be issued on GeM portal and its related documents constitutes the entire agreement between the ERNET India and the contractor. The validity of Contract will be from the date of issue of contract on GeM Portal till the completion of warranty of equipment(s).

2.3 Severability

If any provision or condition of this Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of this Contract.

2.4 Parties

The parties to the contract are the contractor and the ERNET India, as defined in GCC-clause 1.2.

2.5 Contract Documents

The following documents shall be considered to be an integral part of the contract, irrespective of whether these are not appended/ referred to in it. Any generic reference to 'Contract' shall imply reference to all these documents as well:

- 1) Contract issued on GeM Portal.
- 2) Valid and authorized Amendments issued to the contract.
- 3) Final written submissions made by the contractor during negotiations, if any;
- 4) GeM GTC i.e General Terms and Conditions
- 5) GeM (STC i.e Special Terms & Conditions & ATC i.e Additional Terms & Conditions) if any
- 6) the bid document submitted by Bidder;
- 7) Forms and Formats signed and submitted by bidder
- 8) Integrity Pact
- 9) Modifications/ Amendments, Waivers and Forbearances
- 10) Tender Document and its amendment/Corrigendum
- 11) Non-Disclosure Agreement

2.5.1 Modifications/ Amendments of Contract

- 1) If any of the contract provisions must be modified after the contract documents have been signed, the modifications shall be made in writing and signed by the ERNET India, and no modified provisions shall be applicable unless such modifications have

been done. No variation in or modification of the contract terms shall be made except by a written amendment signed by the ERNET India. Requests for changes and modifications may be submitted in writing by the contractor to the ERNET India. At any time during the currency of the contract, the ERNET India may suo-moto or, on request from the contractor, by written order, amend the contract by making alterations and modifications within the general scope of the Contract.

- 2) If the contractor does not agree to the suo-moto modifications/amendments made by the ERNET India, it shall convey its views within 10 days from the date of amendment/ modification conveyed. Otherwise, it shall be assumed that the contractor has consented to the amendment.
- 3) Any verbal or written arrangement abandoning, modifying, extending, reducing, or supplementing the contract or any of the terms thereof shall be deemed conditional and shall not be binding on the ERNET India unless and until the same is incorporated in a formal instrument and signed by the ERNET India, and till then the ERNET India shall have the right to repudiate such arrangements.

2.5.2 Waivers and Forbearances

The following shall apply concerning any waivers, forbearance, or similar action taken under this Contract:

- 1) Any waiver of ERNET India's rights, powers, or remedies under this Contract must be in writing, dated, and signed by an authorized representative of the ERNET India granting such waiver and must specify the terms under which the waiver is being granted.
- 2) No relaxation, forbearance, delay, or indulgence by ERNET India in enforcing any of the terms and conditions of this Contract or granting of an extension of time by ERNET India to the contractor shall, in any way whatsoever, prejudice, affect, or restrict the rights of ERNET India under this Contract, neither shall any waiver by ERNET India of any breach of Contract operate as a waiver of any subsequent or continuing breach of Contract.

3 Governing Laws and Jurisdiction

3.1 Governing Laws and Jurisdiction

- 1) This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Laws of India for the time being in force.
- 2) Irrespective of the location of delivery, or the location of performance or the location of payments under the contract, the contract shall be deemed to have been made at Delhi. The courts of such a location (i.e Delhi) shall alone have jurisdiction to decide any dispute arising out or in respect of the contract.

4 Communications

4.1 Communications

- 1) All communications under the contract shall be served by the parties on each other in writing (Letter/email), in the contract's language, and served in a manner customary and acceptable in business and commercial transactions.
- 2) The effective date of such communications shall be either the date when delivered to the recipient or the effective date mentioned explicitly in the communication, whichever is later.
- 3) No communication shall amount to an amendment of the terms and conditions of the contract, except a formal letter of amendment of the contract, so designated.
- 4) Such communications would be an instruction or a notification or an acceptance or a certificate from the ERNET India, or it would be a submission or a notification from the contractor.

4.2 The person signing the Communications

For all purposes of the contract, there under all communications to the other party shall be signed by:

- 1) The Authorise signatory on behalf of the contractor shall sign all correspondences..
- 2) the Procurement Officer issuing the contract shall administer the contract and sign communications on behalf of the ERNET India. consignees; Project excuting officer; Inspecting officers and the paying authorities mentioned in the contract shall also administer respective functions during Contract Execution.

4.3 Address of the parties for sending communications by the other party.

For all purposes of the contract, including arbitration, thereunder the address of parties to which the other party shall address all communications and notices shall be:

- 1) The address of the contractor as mentioned in the contract unless the contractor has notified the change of address by a separate communication containing no other topic to the ERNET India. The Contractor shall be solely responsible for the consequence of an omission to notify a change of address in the manner aforesaid, and
- 2) The address of the ERNET India shall be the address mentioned in the contract. The contractor shall also send additional copies to officers of the ERNET India presently dealing with the contract.
- 3) In case of the communications from the contractor, copies of communications shall be marked to the Procurement Officer issuing the contract, and as relevant also to Inspecting Officer; Project executing officer; interim/ultimate consignee and paying authorities mentioned in the contract. Unless already stipulated in the contract before the contract's start, the ERNET India and the contractor shall notify each other if additional copies of communications are to be addressed to additional addresses.

5 Contractor's Obligations and restrictions on its Rights

5.1 Changes in Constitution/ financial stakes/ responsibilities of a Contract's Business

The Contractor must proactively keep the ERNET India informed of any changes in its constitution/ financial stakes/ responsibilities during the execution of the contract.

5.2 Obligation to Maintain Eligibility and Qualifications

The contract would be awarded to the contractor based on specific eligibility and qualification criteria. The Contractor is contractually bound to maintain such eligibility and qualifications during the entire duration (including its extensions) of the contract. Any change which would vitiate the basis on which the contract was awarded to the contractor should be pro-actively brought to the notice of the ERNET India within 7 days of it coming to the Contractor's knowledge. These changes include but are not restricted to the Change regarding declarations made by it in its bid in Form 1.2: Eligibility Declarations.

5.3 Consequences of a breach of Obligations

Should the contractor commit a default or breach of GCC-clause 5.1 to 5.6, the Contractor shall remedy such breaches within 21 days, keeping the ERNET India informed. However, at its discretion, the ERNET India shall be entitled, and it shall be lawful on its part, to treat it as a breach of contract and avail any or all remedies thereunder. The decision of the ERNET India as to any matter or thing concerning or arising out of GCC-clause 5.1 to 5.6 or on any question whether the contractor has committed a default or breach of any of the conditions shall be final and binding on the contractor.

5.4 Assignment and Sub-contracting

- 1) All the manpower to be deployed in project for delivery, installation, testing & commissioning and operation & maintenance including onsite support should be on the payroll of the Contractor or OEM whose equipment(s) are offered. Outsourcing of manpower will not be allowed.
- 2) The contractor shall not sublet, transfer, or assign the contract or any part thereof or interest therein or benefit or advantage thereof in any manner whatsoever.
- 3) The contractor shall take prior permission in writing from ERNET India for any sub-contracting that the contractor wish to enter into for limited Works (e.g loading/unloading, racking & stacking of equipment(s), laying of Data Center cabling etc.) .
- 4) If the Contractor sublets or assigns this contract or any part thereof without such permission, the ERNET India shall be entitled, and it shall be lawful on its part, to treat it as a breach of contract and avail any or all remedies thereunder.

5.5 Indemnities for breach of IPR Rights or from other issues

- 1) the contractor shall indemnify and hold harmless, free of costs, the ERNET India and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Equipment provided by the contractor under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or

other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:

- a) any design, data, drawing, specification, or other documents or Equipment provided or designed by the contractor for or on behalf of the ERNET India.
 - b) The installation of the Equipment by the contractor or the use of the Equipment at the ERNET India's / CERT-In/ other end user Sites.
- 2) If any proceedings are brought, or any claim is made against the ERNET India arising out of the matters referred above, the ERNET India shall promptly give the contractor a notice thereof. At its own expense and in the ERNET India's name, the contractor may conduct such proceedings and negotiations to settle any such proceedings or claim, keeping the ERNET India informed.
 - 3) If the contractor fails to notify the ERNET India within twenty-eight (28) days after receiving such notice that it intends to conduct any such proceedings or claim, then the ERNET India shall be free to conduct the same on contractor's behalf at the risk and cost to the contractor.
 - 4) The contractor shall be solely responsible for any damage, loss or injury which may occur to any property or to any person by or arising out the execution of the works or temporary works or in carrying out of the contract otherwise than due to the matters referred to in this agreement hereinbefore. The bidder would ensure for observance of all labour and other laws applicable in the matter and shall indemnify and keep indemnified the ERNET India, end users/ its customers against the effect of non-observance of any such laws.

5.6 Confidentiality and IPR Rights

5.6.1 IPR Rights

All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the contractor under this Contract shall become and remain the property of the ERNET India/ CERT-In and must not be shared with third parties or reproduced, whether in whole or part, without the ERNET India/ CERT-In's prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the ERNET India/ CERT-In, together with a detailed inventory thereof.

5.6.2 Confidentiality

All documents, drawings, samples, data, associated correspondence or other information furnished by or on behalf of the ERNET India/ CERT-In to the contractor, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract, are confidential and shall remain the property of the ERNET India/ CERT-In and shall not, without the prior written consent of ERNET India/ CERT-In neither be divulged by the contractor to any third party, nor be used by him for any purpose other than the design, procurement, or other services and work required for the performance of this Contract. If advised by the ERNET India/ CERT-In, all copies of all such information in original shall be returned on completion of the contractor's performance and obligations under this contract.

5.6.3 Obligations of the contractor

- 1) Without the ERNET India/ CERT-In's prior written consent, the contractor shall not use the information mentioned above except for the sole purpose of performing this contract.
- 2) The contractor shall treat and mark all information as confidential and shall not, without the written consent of the ERNET India/ CERT-In , divulge to any person other than the person(s) employed by the contractor in the performance of the contract. Further, any such disclosure to any such employed person shall be made in confidence and only so far as necessary for such performance for this contract.
- 3) The obligation of the contractor under sub-clauses above, however, shall not apply to information that:
 - a) now or hereafter is or enters the public domain through no fault of Contractor;
 - b) can be proven to have been possessed by the contractor at the time of disclosure and which was not previously obtained, directly or indirectly, from the ERNET India/ CERT-In ; or
 - c) otherwise lawfully becomes available to the contractor from a third party that has no obligation of confidentiality.
- 4) The above provisions shall not in any way modify any undertaking of confidentiality given by the contractor before the date of the contract in respect of the contract/ the Tender Document or any part thereof.
- 5) The provisions of this clause shall survive after completion or termination (for whatever reason) of the contract.

5.7 Performance Bond/ Security

- 1) The successful bidder shall submit a Performance Security @ 3% of total value of Contract within 14 days from the date of issuance of contract. The Performance Security if submitted in the form of Bank Guarantee, Fixed Deposit and Insurance Surety bond should be valid for a minimum period of 46 months (Implementation period+ Warranty Period+ Claim Period of 3 months). The Performance security shall be shall be submitted in one of the following forms:
 - a. Insurance Surety Bonds/ Account Payee Demand Draft/Fixed Deposit Receipt from a Commercial bank/Bank Guarantee from a Commercial bank or online Payment (Account details given below).

1.	Beneficiary Name & Address	ERNET India, 5th Floor, Block I A Wing, DMRC IT Park, Shastri Park, Delhi-110053
2.	Bank Name	Bank of India
3	Bank Branch & Address	Electronics Niketan 6 CGO complex New Delhi
4	Beneficiary Account No	604810100002033
5	IFSC code	BKID0006048

The performance security must be routed through Structured Financial Messaging System (SFMS) from issuing Bank to our Bank as per details given above; by sending IFN 760 COV Bank Guarantee Advice Message.

- b. Bank Guarantee issued by a scheduled commercial bank in India, in the prescribed form provided in Format 1.1.

- 2) If the contractor, having been called upon by the ERNET India to furnish Performance Security, fails to do so within the specified period, it shall be lawful for the ERNET India at its discretion to annul the award and enforce Bid Securing Declaration, besides taking any other administrative punitive action.
 - (a) If the contractor during the currency of the Contract fails to maintain the requisite Performance Security, it shall be lawful for the ERNET India at its discretion to terminate the Contract for Default besides availing any or all contractual remedies provided for breaches/ default, or
 - (b) without terminating the Contract:
 - i. recover from the contractor the amount of such security deposit by deducting the amount from the pending bills of the contractor under the contract or any other contract with the ERNET India, or
 - ii. treat it as a breach of contract and avail any or all contractual remedies provided for breaches/ default.
- 3) Contractor needs to extend the validity of Performance Security as and when asked by ERNET India due to Extension of project timelines or if any other valid reason.
- 4) In the event of any amendment issued to the contract, the contractor shall furnish suitably amended value and validity of the Performance Security in terms of the amended contract within fourteen days of issue of the amendment.
- 5) The ERNET India shall be entitled, and it shall be lawful on his part, to deduct from the performance securities or to forfeit the said security in whole or in part in the event of:

any default, or failure or neglect on the part of the contractor in the fulfilment or performance in all respect of the contract under reference or any other contract with ERNET India or any part thereof for any loss or damage recoverable from the contractor which the ERNET India may suffer or be put to for reasons of or due to above defaults/ failures/ neglect.
- 6) Subject to the sub-clause above, the ERNET India shall release the performance security on completing all contractual obligations at the satisfaction of ERNET India, including the warranty obligations.
- 7) No interest will be payable by ERNET India on any security deposit, amount forfeited, liquidated damages, SLA penalty, amount withheld any delayed payment by ERNET India.

5.8 Permits, Approvals and Licenses

Whenever the supply of Equipment(s) and Services requires that the contractor obtain permits, approvals, and licenses from local public authorities, it shall be the contractor's sole responsibility to obtain these and keep these current and valid.

6 Scope of work, Project Management and Technical Specifications

6.1 Scope of work

- 1) This contract is for the supply, installation, testing & commissioning of equipment(s) of the description, specifications, in the quantities outlined in the contract on or before the dates specified therein.

- 2) Training: Contractor Shall provide the training for installation, operation and maintenance of supplied equipment(s) as detailed in Section-VII.
- 3) **Operation & Maintenance of Equipment(s)** : the contractor shall be required to perform operation(s) and maintenance of supplied and pre-existed Equipment(s) for one year from the respective date of acceptance of project as per specified milestones .
- 4) **Scope of Work detailed as per Section VII**

6.2 Project Planning and Management:

The Contractor is required to design and implement a comprehensive and effective project plan and management methodology using efficient and reliable tools. Project planning exercise shall ideally commence with the start of the project (issue of P.O) and shall continue till the O&M Phase of the project. However, high level project management & planning should commence during the preparation of the bid. To have an effective project management system in place, it is necessary for the Contractor to provide regular project monitoring reports to ERNET India/ CERT-In to monitor the Project Progress at different periodicity basis (during different phases of project) such as daily, weekly and biweekly and monthly basis.

The Contractor shall address at the minimum of the following but not limited to:

- i. Create an organized set of activities for the project;
- ii. Coordinate and collaborate with various stakeholders;
- iii. Establish and measure resource assignments and responsibilities;
- iv. Construct a project plan schedule including milestones, highlighting the dependencies, risks, sub activities wise plan with actions owners per milestone;
- v. Measure project deadlines and performance objectives;
- vi. Communicate the project plan to stakeholders with meaningful reports;
- vii. Provide facility for detecting problems and inconsistencies in the plan;
- viii. Development of Best Practices Document (to be submitted after each milestone, to gather the learnings) and updated version of plan;

During the project implementation, the Contractor shall report the following items to the ERNET India/ CERT-In via the reports:

- i. Results accomplished during the period;
- ii. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalized Project Plan;
- iii. Corrective actions & risk mitigation strategies to be taken to achieve milestones as per planned schedule of progress;
- iv. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the contractor;
- v. Other issues and outstanding problems, and actions proposed to be taken;
- vi. Dependencies resolution plan / Interventions which Contractor expects to be made by ERNET India/ CERT-In and / or actions to be taken by the ERNET India/ CERT-In before the next reporting period. Progress

reports would be prepared by Contractor on a fortnightly basis. These reports may be required to be shared with either the Nodal officer, NRC and ERNET India/ CERT-In, as the case may be;

- vii. Project Quality Assurance;
- viii. Project Management activities;
- ix. Issue Management to help identify and track the issues that need attention and resolution from the ERNET India / Cert-In / Other stakeholders ;
- x. Scope Management to manage the scope and changes through a formal management and approval process;

Risk Management to identify and manage the risks that can hinder the project progress The Project plan prepared by the contractor at the initial stage of the project shall be reviewed by the ERNET India/ CERT-In. The Contractor shall update and maintain the Project Plan throughout the duration of the engagement. All changes are to be reviewed and approved by the ERNET India/ CERT-In or appointed representatives.

Contractor must ensure that a PMP/Prince2 certified with minimum of ten (10) years experience in handling large Data Center project should be nominated as Senior Project Manager who will handle all activities of project (i.e. for implementation and Operation & Maintenance) till its completion. He must be placed in ERNET India/CERT-In office (i.e. at Delhi or Bangalore) as decided by ERNET India and contractor must ensure that person is dedicated for this project only. Contractor shall also ensure that sufficient skilled manpower shall be deployed during implementation and O&M of project in each milestone. Role & Responsibility of Project Head will be:

- Should be responsible for all kind of communications with all the stakeholders of ERNET India/CERT-In ;
- Should be responsible for the project management throughout the entire project lifecycle, including project initiation, project delivery, stakeholder management, post implementation review and project close out / handover;
- Should have to work closely with other team members and Shall be responsible for overall work assigned to Contractor;
- Should be responsible for delivery of all project deliverables as per tender.
- Should provide technical solutions and strategic recommendations to enhance services quality;
- Should communicate technical ideas to technical and non-technical stakeholders. Additionally, the ability to document support procedures to ensure that deployed systems are properly maintained and supported;

Qualification and experience of Senior Project Manager shall be B.E./B.Tech/MCA + 10 Years relevant experience for managing large data centres projects + PMP/Prince2 Certified.

6.3 Technical Specifications and Warranty

The Equipment & Services to be provided by the contractor under this contract shall conform to the technical specifications mentioned in 'Technical Specification' under Sections V of the Tender Document. For standards and requirements where no applicable specifications are mentioned, appropriate latest authoritative standards and quality assurance issued by the concerned institution shall be applicable.

- 1) The Equipment supplied shall be entirely brand new and unused.
- 2) The Equipment(s) specifications provided in the tender is the minimum required and bidder may quote for higher specifications to optimize as per their solution requirements. The bidders should quote the products strictly as per the tendered specifications or of higher specifications giving exact make & model and specifications. All the technical literature for the products offered by the bidder may be enclosed in the bid.
- 3) The bidders should give clause-by-clause compliance for the technical specification of the equipment along with cross reference of individual points from product data sheet/ literature which is to be submitted in their technical bids.
- 4) Bidders must provide make and model of offered equipment etc. as per Form 3A i.e Unpriced Make and Model of Offered Equipment(s) compliance.

6.4 Warranty

The following warranty clauses shall apply:

- 1) The Equipment supplied and services rendered by the contractor shall be in accordance with the tender specifications. The Contractor shall carry onsite comprehensive Warranty for Three (3) year for all supplied equipment(s) and software. The warranty period shall start from the respective date(s) of successful commissioning by contractor and acceptance by ERNET India of each milestone.
- 2) Obligations of the contractor under the warranty clause shall remain valid for all the sites installed, accepted and paid-for; even though the contract is terminated for any reason whatsoever.
- 3) OEM Warranty certificates must be submitted by Contractor at the time of delivery of Equipment. For the intervening period between Date(s) of Delivery and Date(s) of acceptance, the Contractor shall get the warranty extended from OEM and shall submit necessary document proof in this regard at the time of submission of invoice(s).
- 4) Warranty should reflect in the support website of the OEM if such option is provided by the respective OEMs
- 5) The equipment to be ordered through the Contract/P.O are meant to be deployed across various location across the country. In case any of the installed/ non-installed equipment(s) are shifted from one location to another then the contractor shall be responsible to provide warranty, support, maintenance and RMA (Return Merchandise Authorization) at such locations also.
- 6) **Retention Policy:** Since the equipment(s) to be deployed in security projects; therefore data privacy shall be ensured through Storage Retention Policy i.e. ERNET

India/CERT-In shall retain the faulty storage disks/media/memory in case of any replacement during the maintenance. In case of replacement of any device/equipment, ERNET India/CERT-IN shall retain all the storage disks (faulty or otherwise). No additional cost will be paid for any retained storage disks.

- 7) In case of any rectification of a defect or replacement of any defective Equipment during the warranty period, the warranty for the rectified/ replaced Equipment shall remain till the original warranty period and same should reflect on OEM's website with revised equipment details, if such facility available with OEM.
- 8) All ongoing software upgrades, patches for all major and minor releases should be provided during the warranty period.
- 9) OEM support should be provided on all days and at all hours.
- 10) All types of support (hardware/software trouble shooting, maintenance etc.) at Central (DC/DR) & remote locations will be provided by the contractor.
- 11) The Contractor shall arrange for free Onsite comprehensive maintenance for a period of warranty from the date/dates of acceptance of the project milestone wise with regard to rectification/removal of defects if any observed during this period. If the Contractor does not arrange to rectify the defects observed during the maintenance period within a reasonable time (10 days), the ERNET/End user shall be at liberty to get such defects rectified at the cost and risk of the Contractor in addition to levying of penalties.

12) SLA during warranty period and penalties thereof:

- i. During Operation & Maintenance (O&M), Service levels defined under Section VIII will be applicable.
- ii. After completion of O&M of 1 year (during the warranty period), Bidder will deploy two resident engineers (One for Networking & One for System/Server) in each shift (total 3 shifts per day 8 hours each shift) at each Data Center (DC & DR) and restore the Equipment & services within 24 hours (i.e. the permissible limit) of the failure. Resident Engineer must be OEM certified for networking & Systems with at least 3 years of relevant experience and must possess BE/B.Tech/MCA degree. Document proof shall be submitted at the time of deployment of such resident engineer.
- iii. Remote site equipment(s) will be managed by Contractor's own manpower operating from its own offices.
- iv. In the absence of Manpower at DC and DR, Penalty of Rs. 1000 per day of absence per manpower will be imposed. In case of absence of both the manpower at any of the locations (DC and DR), A penalty of Rs. 5,000 per day of absence per manpower will be imposed. Further if the above situation persists for more than 7 days, ERNET India may initiate termination clause for default.
- v. At Data Center (DC & DR) and remote Sites, for faults in equipment under warranty, Penalty @ 0.25 % of equipment cost of the affected portion* per day or or part thereof will be deducted beyond permissible limits. In case fault persists for more than 2 days, then Penalty @ 0.1 % of equipment cost of the affected portion* per hour will be deducted.

- vi. Penalty of Rs.1000 on per 24-hour basis will be charged for equipment whose price could not be derived from the price bid besides the penalty arising out the affected portion* per hour.
- vii. If the contractor, having been notified, fails to rectify/ replace the defect(s) within 10 days, it shall amount to breach of Contract for default, and the ERNET India may avail any or all remedial action(s) mentioned under termination clause for default.
- viii. During warranty period after O&M, bidder must do preventive maintenance (PM) for DC & DR at a frequency of 6 months and once in a year for each remote site. If PM is missed as per defined frequency, the same should be carried out within next four weeks. Else penalty of Rs. 50,000/- per day or part thereof per data centre(DC/DR) and Rs. 5,000/- per day or part thereof per remote site for delays will be deducted.
- ix. No penalty will be imposed for downtime asked by the bidder for preventive maintenance, patch upgradation etc. However, any of these activity shall be done only in off peak hour and after taking due permission from CERT-In.
- x. Penalties will be deducted from due payment/performance securities.
- xi. The overall Penalties for non-adherence with the SLA of warranty support (during 2nd & 3rd year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2.

***Affected portion means:** If any equipment down and other hardware which were not in service due to failure of main equipment. e.g If both leaf switch are down and due to that complete server rack is down then penalty will be imposed on all equipment falling in that particular rack. Similar penalty calculation w.r.t affected portion will be followed for all type of equipment installed in this project including intelligent cabling.

7 Inspection and Quality Assurance

7.1 Tests and Inspections

ERNET India or its representative shall have the right to inspect or to test the Equipment(s) to confirm their conformity to the ordered specifications. The contractor shall provide all reasonable facilities and assistance to the inspecting authority at no charge to ERNET India. In case any inspected or tested equipment fail to conform to the specifications, ERNET India may reject them and contractor shall replace the rejected equipment with the equipment in conformity with the specification required free of cost to ERNET India.

7.2 Consequence of Rejection

Upon the Equipment being rejected by the ERNET India, the ERNET India shall be at liberty to demand that such equipment(s) shall be removed and replaced with a brand new equipment by the contractor at his cost subject as hereinafter stipulated, within 15 days from the date of intimation of such rejection. The decision of the ERNET India for rejection shall be final in all respects. The Contractor shall bear all cost of such replacement, including taxes and freight, if any, on replacing and replacing Equipment without being entitled to any extra payment on that or any other account. ERNET India/CERT-In will not return the Hard Disk from used systems. Replaced equipment shall have same or higher specifications. Contractor shall provide the replacement

within a maximum of 30 days, if contractor fails to do so , then it will be treated as breach of contract as per clause 12.1 and accordingly remedial action may be initiated.

7.3 ERNET India's right of Rejection of Inspected Equipment

- 1) Equipment accepted by the ERNET India after inspection in terms of the contract shall in no way dilute the ERNET India's right to reject the same later if found deficient concerning 'Technical Specifications'.
- 2) Notwithstanding any approval which the ERNET India may have given in respect of the Equipment or any materials or other particulars or the work or workmanship involved in the performance of the contract and notwithstanding delivery of the Equipment, it shall be lawful for ERNET India, to inspect, test and, if necessary, reject the Equipment or any part, portion or consignment thereof, after the Equipment's arrival at the final destination within a reasonable time after actual delivery thereof at the delivery locations mentioned in the contract, if such Equipment or part, portion or consignment thereof is not in all respects in conformity with the terms and conditions of the contract whether on account of any loss, deterioration or damage before despatch or delivery or during transit or otherwise howsoever.

8 Transfer of Assets and Insurance

8.1 Transfer of Assets

The ownership of the supplied Equipment along with its warranty and all other associated rights shall be transferred within 90 days to CERT-In, ; after successful Commissioning and Acceptance of each milestone by ERNET India. All the risks, responsibilities, liabilities thereof in respect of all equipment shall remain with contractor till acceptance of each milestone. All licenses are to be provided in the name of **Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology Government of India**. Contact details including email id of Cert-In will be provided to L-1 bidder. Contractor shall provide following documents during handover of assets as per milestones:

- 1) Invoices with serial no of devices
- 2) Bill of Material
- 3) OEM Warranty certificates
- 4) Duly received Delivery challan at all locations
- 5) Software license detail, if any
- 6) Final Acceptance report
- 7) Any other document specified by ERNET India

8.2 Insurance

The Bidders shall also arrange to get equipment insured to cover loss/damage due to theft, burglary, fire, or any natural disaster for the period till 30 days after successful acceptance as per respective milestones as defined in terms of delivery in this tender document. Bidder shall be required to extend the insurance period in case, there is delay in commissioning & acceptance of project. The insurance shall not be for an amount less than 100 percent of the

value of the equipment(s) as mentioned in the contract. Bidder may include cost of insurance in the unit price of equipment(s) quoted in the price bid.

9 Terms of Delivery and delays

9.1 Effective Date of Contract

The effective date of the contract shall be the date on which it has been issued by issued by GeM Portal. The dates of deliveries shall be counted from the date of contract.

9.2 Place (destination/Location) of Delivery

The city of sites (remote/DC/DR) where the Equipment are to be delivered have been stipulated in the Section IV – Bill of Material.

9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance

1. All Equipment & Services shall be offered at site including logistics, transportation, loading/unloading, installation, testing & commissioning. Cost of the same may be included in offer price. All aspects of safe delivery shall be the sole responsibility of the bidder.
2. Any changes in end user locations shall also be confirmed at the time of release of Contract. Contractor should obtain list of end user locations from ERNET India at the time of issuance of Contract and adhere to the same. ERNET India reserve the right to change the location before delivery of Equipment(s) to designated locations without paying any additional cost for the same. However, any relocation of equipment(s) in the same city shall not be treated as change of location before equipment(s) installation. No Equipment shall be deliverable to the ERNET India/CERT-In on Sundays and public holidays or outside designated working hours without the written permission of ERNET India/CERT-In.
3. The contractor shall deliver the consignment at the location(s) as detailed in the Bid/contract, the quantities of the Equipment detailed therein, and the Equipment shall be delivered not later than the dates stipulated in the tender/contract. The delivery shall not be complete unless the Equipment are inspected and accepted by the ERNET India/CERT-In as provided in the contract.
4. In case the Contractor fails to despatch the Equipment before the expiry of the delivery period then bidder must apply to ERNET India in writing to extend the delivery period and only if approved by the ERNET India then only dispatch the balance quantity in specified delivery time limit. If the bidder despatches the Equipment without obtaining an extension, it would be doing so at its own risk, and no claim for payment for such supply and/ or any other expense related to such supply shall lie against ERNET India.
5. Location of sites which are to be covered in the respective milestone as defined in timeline for delivery table (below) will be provided by ERNET India in consultation with CERT-In to successful bidder.
6. **Timeline for Delivery, Installation, testing, commissioning & Acceptance:**

Sl. No.	Activity	Timeline (Milestone)	Project Milestones
1	Date of issue of contract. This is being referred as "T" in the timeline column of this table.	T	Start of Milestone-1
2	Site Survey of Data Centre(DC) & 50 remote sites for readiness assessment for deployment of Infrastructure by Contractor in coordination with ERNET India/CERT-In.	T+8 Weeks	
3	Delivery of Complete Hardware at Data Centre	T+16 Weeks	
4	Installation, Testing & Commissioning of Complete Hardware, (as mentioned at S.No#3) Delivery, Installation, Testing & Commissioning of Complete Hardware at 50 remote sites. EMS & DCIM Solution and their integration with existing Phase-1 Hardware & MPLS links including Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP) .	T+20 Weeks	
5	Acceptance by ERNET India of Complete Milestone-1 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+24 Weeks	Completion of Milestone-1
6	Site Survey, Delivery, Installation, Testing & Commissioning of Complete Hardware at another 50 Remote Sites and their integration with DC's EMS,DCIM Solution, including Offering of this infrastructure under Milestone-2 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP)	T+26 Weeks	Start of Milestone-2
7	Acceptance by ERNET India of Complete Milestone-2 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+28 Weeks	Completion of Milestone-2
8	Site Survey , Delivery, Installation, Testing & Commissioning of Complete Hardware at another 50 Remote Sites and their integration with DC's EMS,DCIM Solution, including Offering of this infrastructure under Milestone-3 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP)	T+26 Weeks	Start of Milestone-3
9	Acceptance by ERNET India of Complete Milestone-3 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+28 Weeks	Completion of Milestone-3
10	Site Survey , Delivery of Complete Hardware of Data Recovery Centre (DR). This will be called as start of Milestone-4.	T+22 Weeks	Start of Milestone-4
11	Installation, Testing & Commissioning of Complete Hardware (as mentioned at S.No#10) , EMS & DCIM Solution and their integration with DC, DC's EMS,DCIM	T+26 Weeks	

	Solution & also integration of accepted remote sites(which were connected with DC over IPSEC tunnels)with DR Infrastructure over MPLS links including Offering of this infrastructure under Milestone-4 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP).		
12	Acceptance by ERNET India of Complete Milestone-4 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+28 Weeks	Completion of Milestone-4
13	Site Survey , Delivery, Installation, Testing & Commissioning of Complete Hardware at another 50 Remote Sites and their integration with DC's EMS,DCIM Solution, including Offering of this infrastructure under Milestone-5 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP)	T+26 Weeks	Start of Milestone-5
14	Acceptance by ERNET India of Complete Milestone-5 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+28 Weeks	Completion of Milestone-5
15	Site Survey , Delivery, Installation, Testing & Commissioning of Complete Hardware at another 32 Remote Sites and their integration with DC's EMS,DCIM Solution, including Offering of this infrastructure under Milestone-6 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP)	T+26 Weeks	Start of Milestone-6
16	Acceptance by ERNET India of Complete Milestone-6 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+28 Weeks	Completion of Milestone-6

Note : “EMS & DCIM Solution” refers to Data Center Infrastructure Management (DCIM), RF Id Based Physical Asset Tracking & Heat Humidity Sensor Solution , EMS Solution with all its modules along with IT helpdesk / service desk and IPAM/Switch Port Management in High Availability mode.

Completion of Milestone-1 is mandatory before other milestones, without which, other milestones won't be treated as completed. However, ERNET India reserves the right to change the schedule of delivery of equipment in each milestone as per project requirement. Contractor must ensure continued satisfactory performance of the previously accepted milestones while offering for the acceptance of subsequent milestones.

Timeline for Operation & Maintenance (O&M) after acceptance of individual milestones.

Sl. No	Activity	Expected time to begin O&M (Milestone)	Completion of O&M
1	O&M of Milestone 1	T+24 Weeks	

2	O&M of Milestone 2	T+28 Weeks	O&M in respect of all the Milestones for one year
3	O&M of Milestone 3	T+28 Weeks	
4	O&M of Milestone 4	T+28 Weeks	
5	O&M of Milestone 5	T+28 Weeks	
6	O&M of Milestone 6	T+28 Weeks	

9.4 Delay in the contractor's performance

If the contractor fails to deliver the Equipment(s) or any instalment thereof or delays in provision of Services (e.g. delivery, installation, commissioning, training, O&M etc.) within the period fixed for such delivery in the contract or as extended or at any time repudiates the contract before the expiry of such period, the ERNET India may without prejudice to Contractor's other rights:

- 1) recover from the contractor liquidated damages as per clause 9.5(2) below, or
- 2) treat the delay as a breach of contract as per clause 12.1 below and avail all the remedies therein.

9.5 Extension of Delivery Period and Liquidated Damages:

ERNET India may, on the request of the bidder or otherwise, extend the delivery date suitably subject to the following conditions:

- 1) The original Delivery Period may be re-scheduled by the ERNET India without any Liquidated damages if such reschedule is warranted due to Force Majeure conditions mentioned below and also on the ground/reasons of delay attributable to the ERNET India. In all other cases, if any extension is given then same shall also attract LD as given in clause 9.5.2 below.
- 2) **Liquidated Damages (LD):** If the Contractor fails to meet the prescribed timelines, starting from delivery of complete hardware under respective milestones, for any reason whatsoever then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay @ 1 % of the Contract value of the respective milestone per week or part of the week of delayed period. Overall Liquidated Damages shall not exceed 10% of the contract value (including taxes). In case, delay beyond 10 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.
- 3) In case the Contractor completes the respective milestone(s) within the overall timelines specified for completion of that milestone then no LD will be levied for any intermediary delay in completion of any of the stages of the respective milestones.
- 4) ERNET India will serve a notice duly accompanied by a preliminary calculation sheet to the contractor against whom levy of LD is proposed. In case the contractor is not satisfied/ agrees with :
 - (i) the reason/grounds for which leaving of LD is proposed and
 - or
 - (ii) method of calculation of amount of LD.

then Contractor may submit a written representation to ERNET India within the stipulated timeline (as indicated in the notice i.e. 15 days) clearly mentioning his claims, ground of such claims etc. along with all the documents (self-certified) supporting his claims. The decision of DG, ERNET India shall be final and binding in this matter.

- 5) Waiver from LD may be considered only if the contractor submits a written representation to ERNET India within the stipulated time (as indicated in the notice i.e. 15 days) on receipt of such notice of imposition of LD issued by ERNET India. Decision of ERNET India in the matter shall be final and binding.

9.6 Force Majeure:

- 1) On the occurrence of any unforeseen event, beyond the control of either Party, directly interfering with the delivery of Equipment(s) and Services arising during the currency of the contract, such as war, hostilities, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts, or acts of God, the affected Party shall, within a week from the commencement thereof, notify the same in writing to the other Party with reasonable evidence thereof. Unless otherwise directed by ERNET India in writing, the contractor shall continue to perform its obligations under the contract as far as reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. If the force majeure condition(s) mentioned above be in force for 90 days or more at any time, then in such a case either party shall have the option to terminate the contract on expiry of 90 days of commencement of such force majeure by giving 14 days' notice to the other party in writing. In case of such termination, no damages shall be claimed by either party against the other, save and except those which had occurred under any other clause of this contract before such termination.
- 2) Notwithstanding the remedial provisions contained in GCC-clause 9.6 (2) or 12.1.1, none of the Party shall seek any such remedies or damages for the delay and/ or failure of the other Party in fulfilling its obligations under the contract if it is the result of an event of Force Majeure.

10 Prices and Payments Terms:

1. Payments to Contractor shall be made through EFT only. The Contractor shall provide necessary information/documents for receipt of payment through EFT.
2. Any payment shall be subject to submission of performance security in line with the requirements specified under the Performance Security Clause. Payments shall only be made in Indian Rupees.
3. The contractor shall submit its claim for payment in writing along with relevant supporting documents, as stipulated in Contract and in the manner as also specified herein.
4. The documents which the contractor is to furnish while claiming payment after are:

- a. Original Invoice (GST Compliant format) with serial no of each item.
- b. Delivery challan duly received (sign & Stamped from concerned officer) for all locations
- c. License (software & Hardware)
- d. Warranty document from OEM
- e. Certificate of Insurance till the time of commissioning & acceptance period as detailed in tender.
- f. Successful Commissioning and Acceptance report also to be submitted for claiming the payment after commissioning.
- g. Attendance Sheet of Manpower duly signed & Stamped by the Contractor.
- h. Any other document specified by ERNET India during the course of project.

5. The payment terms are:

- a. Under this project, there are two types of Payments. One is CAPEX Payment i.e. price of equipment(s) and other is payment pertaining to OPEX i.e. Operation & Maintenance (O&M) services.
- b. In respect of DC and DR equipment (s), 50% of the total value of equipment(s) delivered at DC and similarly 50% of the total value of equipment(s) delivered at DR shall be released on 100% of delivery of all equipment(s) in good condition based on the respective milestone(s) and after successful Rack mounted, Power on Self-Test (PoST) by the Contractor.
- c. In respect of equipment (s) at DC and DR, additional 35% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).
- d. In respect of equipment at remote sites, 85% of the total value of items will be made after successful delivery, installation, integration, commissioning and acceptance the respective milestone(s).
- e. Thereafter, based on successful performance during warranty period, balance 15% value of the respective milestone shall be released in twelve (12) equal instalments on a quarterly basis after completion of every quarter. It would be duty of contractor to get the satisfactory performance certificate from CERT-In or (any other 3rd party to whom equipment's warranty has been transferred on the basis of instructions from ERNET India) along with necessary documents. ERNET India may give an option to contractor to claim Balance 15% payment against submission of Bank Guarantee. If this option is given by ERNET India and the same is accepted by Contractor, then the contractor would be having an option to submit Bank Guarantee (BG) for: -
 - i. 15% value, with the validity till completion of warranty period of last milestone + Three (3) months of claim period, or
 - ii. Three (3) Bank Guarantees of 5% each (as reduced by the payment (s) already made w.r.t warranty and maintenance support) valid for one year, Two year & Three years from the date of last milestone + 3 months of claim period.
 - iii. Bank Guarantee formats and required undertaking to be signed by the contractor in this respect will be given to contractor at the time of exercising this option.
- f. O&M Charges (OPEX Charges) during Operation & Maintenance for Data Centres (DC & DR) and Remote Sites will be released on quarterly basis after completion of each quarter from the date of acceptance of respective milestone..

- g. O&M Charges for remote sites will start from the completion of respective milestone and will be paid proportionately based on O&M price derived for each site from price bid.
- h. ERNET India will deduct LD and/or SLA penalty and/or other recoveries (if any) before releasing any payments. In case ERNET India allows the option to submit the BG for balance 15% , SLA penalty and/or other recoveries (if any) shall be required to be paid by the contractor within 30 days from the date of intimation sent by ERNET India in this regard , else same will be recovered by invoking the submitted BGs.
- i. If anytime , ERNET India invokes the submitted BG as per clause 10(5)(e) above (B.G, Insurance Bonds FD, etc.) then amount remaining balance after recovery of dues will be kept by ERNET India and balance will be refunded after completion of validity period of the BG that has been invoked.
- j. Payment of Delivered quantities if it exceeds the quantities mentioned shall be restricted to quantities mentioned in the contract.

11 Arbitration

- 1) In case any dispute or difference arises out of or in connection with or the carrying out of works (whether during the progress of the works or after their completion & whether before or after the termination, abandonments or breach of contract) except as any of the accepted matters, provided hereunder, the parties hereto, shall first endeavour to settle such disputes of differences amicably.
- 2) If both the parties fail to reach such amicable settlement, then either party (The Purchaser or Contractor) may (within 20 days of such failure) give a written notice to the other party requiring that all matter in dispute or difference be arbitrated upon. Such written notice shall specify the matters which are in difference or differences of which such written notice has been given and no other shall be reoffered to the arbitration of a single arbitrator, to be appointed by both the parties or in case of disagreement as to the appointment of a single arbitrator, to that of two arbitrators, one to be appointed by each party or in case of said arbitrators not agreeing then, to the umpire to be appointed by the arbitrators in writing before entering upon the references. Provisions of Indian Arbitration & Conciliations Act, 1996 or any statutory modification or re-enactment thereof and rules framed there under from time to time shall apply to such arbitration.
- 3) Venue of arbitration shall be New Delhi.
- 4) The arbitrators or arbitrators appointed under this Article shall have the power to extend the time to make the award with the consent of parties.
- 5) Pending reference to arbitration, the parties shall make all endeavors to complete the work in all respect. The disputes, if any, will finally be settled in the arbitration.
- 6) Upon every or any such references to the arbitration, as provided herein the cost of and incidental to the reference and Award respectively shall at the discretion of the arbitrator, or the umpire, as case may be.
- 7) The award of arbitrator or arbitrators, as the case may be, shall be final and binding on the parties. It is agreed that the contractor shall not delay the carrying out of the works

by reason of any such matter, question or dispute being referred to arbitration, but shall proceed with the works with all due diligence. The Purchaser and the contractor hereby also agree that arbitration under this clause shall be the condition precedent to any right of action under the contract except for as provided for in the Tender.

12 Defaults, Breaches, Termination, and closure of Contract

12.1 Termination due to Breach, Default, and Insolvency

12.1.1 Defaults and Breach of Contract

In case the contractor undergoes insolvency or receivership; neglects or defaults, or expresses inability or disinclination to honour his obligations relating to the performance of the contract or ethical standards or any other obligation that substantively affects the ERNET India's rights and benefits under the contract, it shall be treated as a breach of Contract. Such defaults could include inter-alia:

- 1) **Default in Performance and Obligations:** if the contractor fails to deliver any or all of the Equipment(s) and services or fails to perform any other contractual obligations (including obligation to maintain eligibility and Qualifications based on which contract was awarded) within the period stipulated in the contract or within any extension thereof granted by the ERNET India.
- 2) **Insolvency:** If the contractor shall at any time, be adjudged insolvent or shall have a receiving order or order for the administration of his estate made against him or shall take any proceeding for composition under any Insolvency Act for the time being in force or make any conveyance or assignment of his effects or enter into any assignment or composition with his creditors or suspend payment, or
- 3) **Liquidation:** if the contractor is a company being wound up voluntarily or by order of a Court or a Receiver, Liquidator or Manager on behalf of the Debenture-holders is appointed, or circumstances shall have arisen which entitle the Court or Debenture-holders to appoint a Receiver, Liquidator or Manager.

12.1.2 Notice for Default:

As soon as a breach of contract is noticed, 'Notice of Default' shall be issued to the contractor, giving two weeks' time to resolve the issues mentioned in the notice. Despite serving NFD, ERNET India would be having right to invoke contractual remedies to safeguard its interest.

12.1.3 Terminations for Default

- 1) **Notice for Termination for Default:** In the event of unsatisfactory resolution of 'Notice of Default' within two weeks of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.
- 2) Such termination shall not prejudice or affect the rights and remedies, including under sub-clause below, which have accrued and/ or shall accrue to the ERNET India after that.
- 3) Unless otherwise instructed by the ERNET India, the contractor shall continue to perform the contract to the extent not terminated.
- 4) All warranty obligations, if any, shall continue to survive despite the termination.

12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default

If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then ERNET India may take any one; or more of the following contractual remedies.

- 1) Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete.
- 2) Recover liquidated damages for delays.
- 3) Encash and/ or Forfeit performance or other contractual securities.
- 4) Debar the contractor from participation in future procurements as follows:

ERNET India may debar the contractor or any of its successors from participating in any Tender Process undertaken by all its procuring entities for a period not exceeding two years commencing from the date of debarment

- 5) Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause.
- 6) **Risk and Cost Procurement:** In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It shall, however, be at the discretion of the ERNET India to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.

Note: Regarding the Equipment which are not readily available in the market and where procurement difficulties are experienced, the period for making risk procurement shall be twelve months instead of nine months provided above.

- 7) Initiate proceedings in a court of law for the transgression of the law, tort, and loss, not addressable by the above means.

12.1.5 Limitation of Liability

Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.

12.2 Termination for Default/ Convenience of ERNET India

12.2.1 Notice for Determination of Contract

- 1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor at any time during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.
- 2) Such termination shall not prejudice or affect the rights and remedies accrued and/ or shall accrue after that to the Parties.
- 3) Unless otherwise instructed by the ERNET India, the contractor shall continue to perform the contract to the extent not terminated.
- 4) All warranty obligations, shall continue to survive despite the termination.

12.3 Closure of Contract

12.3.1 No Claim Certificate and Release of Contract Securities

After mutual reconciliations of outstanding payments and assets on either side, the contractor shall submit a 'No-claim certificate' to the ERNET India requesting the release of its contractual securities, if any. The ERNET India shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the contractor. The contractor shall not be entitled to make any claim whatsoever against the ERNET India under or arising out of this Contract, nor shall the ERNET India entertain or consider any such claim, if made by the contractor, after he shall have signed a "No Claim" Certificate in favour of the ERNET India. The Contractor shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof.

12.3.2 Closure of Contract

The contract shall stand closed upon

- 1) Successful performance of all obligations by both parties, including completion of warranty obligations and final payment.
- 2) termination and settlements after that, if any, as per clause 12.1 or 12.2 above.

Section IV: Bill of Material

Note for Bidders: Regarding this Schedule, Bidders must fill Form 2: 'Bill of Material - Compliance' with their Technical bid.

Part A							
Sl. No.	ITEM	Equipment Quantity at DC	Equipment Quantity at DR	Equipment Quantity at Remote	Equipment Quantity at New Delhi	Total Quantity	Unit of Measurement
1	Server Category-1	115	50	0	0	165	no.
2A	Server Category-2 (4U) with 60 HDD in Each Server	425	100	0	0	525	no.
2B	Server Category-2 (6U) with 84 HDD in Each DAS	304	72	0	0	376	no.
3	Server Category-3	20	10	0	0	30	no.
4	Server Category-4	20	10	0	0	30	no.
5	Server Category-5	10	5	0	0	15	no.
6	Server Category-6	0	0	200	0	200	no.
7	Server Category-7	0	0	6	0	6	no.
8	Server Category-9	0	0	20	0	20	no.
9	Server Category-10	0	0	16	0	16	no.
10	Server Category-11	6	6	0	0	12	no.
11	Server Category-13	6	2	0	0	8	no.
12	Server Category-14	0	2	0	0	2	no.
13	Server Category-16	0	2	0	0	2	no.
14	DC Spine Switch	0	2	0	0	2	no.
15	DC Leaf Switch	50	60	0	0	110	no.
16	DC Core Switch	2	2	0	0	4	no.
17	DC OOB Access Switch	80	60	0	0	140	no.
18	Layer-3 Access Switch	10	10	0	0	20	no.
19	DC CE Router	0	2	0	0	2	no.
20	DC Border Leaf Switch	0	2	0	0	2	no.
21	DC Internet Router	0	2	0	0	2	no.

22	DC Interconnect Switch - Type 1	0	2	0	0	2	no.
23	DC Interconnect Switch - Type 2	0	2	0	0	2	no.
24	DC WAN Switch	0	2	0	0	2	no.
25	SFP-10G-SR4*	3000	3200	0	0	6200	no.
26	SFP-10G-LR4*	50	50	0	0	100	no.
27	QFSP 28 -SR4*	225	625	0	0	850	no.
28	QFSP-28-LR4*	5	5	0	0	10	no.
29	Remote Router cum Firewall	0	0	232	8	240	no.
30	Internet Firewall with IPS	0	2	0	0	2	no.
31	DC Internal Firewall	0	2	0	0	2	no.
32	DC Solution Firewall	0	2	0	0	2	no.
33	AAA Appliance	0	2	0	0	2	no.
34	Load balancer	0	2	0	0	2	no.
35	Network Detection & Response (NDR)	1	1	0	0	2	no.
36	IPS&IDS	2	2	0	0	4	no.
37	SSL VPN Gateway	2	2	0	0	4	no.
38	Active Directory Solution	2	2	0	0	4	no.
39	Console management server	2	2	0	0	4	no.
40	KVM Console	40	20	0	1	61	no.
41	Portable KVM console adapter	5	5	0	5	15	no.
42	Monitoring and management tool for servers	1	1	0	0	2	no.
43	Fireproof Vault (200litre)	1	1	0	2	4	no.
44	Degausser	2	1	0	2	5	no.
45	Data Diode *	0	0	10	0	10	no.
46	Intelligent Cabling (includes all required accessories briefed in specs for 70 Racks in DC)#.	1	0	0	0	1	no.
47	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 70 Racks in DC . One Monitor can maximum monitor 2 Racks	35	0	0	0	35	no.
48	Intelligent (AIM) system Software for 15k Ports in DC	1	0	0	0	1	no.

49	Intelligent Cabling (includes all required accessories briefed in specs for 50 Racks in DR)# - Specifications similar to s.n. 46	0	1	0	0	1	no.
50	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 50 Racks in DR . One Monitor can maximum monitor 2 Racks- Specifications similar to s.n. 47	0	26	0	0	26	no.
51	Intelligent (AIM) system Software for 10k Ports in DR-Specifications similar to s.n. 48	0	1	0	0	1	no.
52	Smart Single Rack (minimum usable space 24U)*	0	0	9	1	10	no.
53	Non Smart Rack with Redundant IPDU*	0	0	5	0	5	no.
54	65 Inch LED Display	1	1	0	0	2	no.
55	Heavy Duty Workstation	25	10	0	0	35	no.
56	Heavy Duty Laptop	10	10	0	10	30	no.
57	Heavy Duty Color Printer	1	1	0	2	4	no.
58	Privileged Access Manager (in HA Mode)	2	0	0	0	2	no.
59	Any other Item						

**Items may increase or decrease as per site requirement assessed by Bidder.*

#Further if server racks increase then value of cabling per rack will be deduced by 'value quoted for 70 racks' divided by 70 and for DR it will be 'value quoted for 50 racks' divided by 50. For DC , Maximum rack extension may go upto 85 and for DR it may go upto 60 Racks.

Part B

S/N	Item	DC	DR	Total Qty	Unit of Measurement
1	Data Center Infrastructure Management (DCIM), RF Id Based Physical Asset Tracking & Heat Humidity Sensor Solution				

1.a	Supply, Installation , Commissioning & Testing (SITC) of following: i) DCIM, ii) RF based Physical Asset Tracking Solution and iii) Heat-Humidity Sensor Solution with respective hardware (servers) in a High Availability mode & overall integration as per scope of work & technical specs. Perpetual Licenses for above solutions for the below stated hardware:	1	1	1 (both working together to form HA mode*)	set
	Number of Racks at DC = 100				
	Number of Racks at DR = 50				
	Total IT active devices at DC = 1450 , Total IT active devices at DR = 350				
	* Note: SI must refer to scope of work & technical specs & accordingly provide one instance of solution at DR .				
1.b	RF Id based Physical Asset Tracking Tags with one on each IT Element (Network/servers) at DC & DR as per scope of work & technical specs.	1450	350	1800	nos.
1.c	RF Id Rack Identifiers as a part of Physical RF Id based Asset Tracking Solution at DC & DR .	100	50	150	nos.
1.d	RF Id Based Heat and Humidity Sensors for Racks at DC & DR as per scope of work & technical specs. Note: should include sensors tags for Phase-1 equipment(s) at DC as well.	300	150	450	nos.
1.e	1. Communication Gateways for Communication on RF with Asset and Heat-Humidity tags & on ethernet/WiFi with respective Software Solution at DC and DR (Based on number of Asset and Heat- Humidity sensors provided.)#	1 Set	1 Set	2	set
	2. Compatible Handheld scanner to read barcode / QR codes at DC & DR				

	3. Barcode Printer / QR codes with consumables(3Yrs Duration) at DC & DR				
2	EMS Solution (SITC of EMS (fault, performance , configuration , change , event ,traffic, asset, SLA management, IT helpdesk / service desk and IPAM functionality along with respective hardware (servers)) in High Availability mode & including the overall integration as per scope of work & technical specs.) * Note: SI must refer to scope of work & technical specs & accordingly provide one instance of solution at DR .	1	1	1 (both working together to form HA mode*)	set
	Note : Solution must maintain historical data for 1 year, has an integrated syslog to acts as a sysLog aggregator.				
	For details refer tech specs and Scope of work.				
	Total IT Elements = 2800 , For 50 Concurrent Users				
	For monitoring of MPLS Link of 250 locations				
3	Additional EMS License Price for 50 IT devices			50	lot
4	Additional IT Helpdesk/EMS License for 5 concurrent users			5	lot
5	Additional DCIM User License price for 5 concurrent users.			5	lot
6	Additional DCIM License price for 5 Racks			5	lot

Part C	
S/N	Item
	Operation and Maintenance for DC, DR and Remote Sites
1	Operation and Maintenance (O&M) of DC along with deployment of 20 Technical Manpower at DC
2	Operation and Maintenance of DR along with deployment of 14 Technical Manpower at DR
3	Operation and Maintenance of Remote Sites
4	Deployment of 2 Technical Manpower for Technical Support at Delhi

Cities where Hardware to be delivered:

S/N	Sites	City		S/N	Sites	City
1	DC	Bangalore		23	Remote	Bangalore
2	DR	Mohali		24	Remote	Bhopal
3	Remote	Kollam		25	Remote	Bhubneshwar
4	Remote	New Delhi		26	Remote	Chandigarh
5	Remote	Mumbai		27	Remote	Chennai
6	Remote	Chennai		28	Remote	Noida
7	Remote	Bangalore		29	Remote	Hyderabad
8	Remote	Chennai		30	Remote	Jammu
9	Remote	Chennai		31	Remote	Lucknow
10	Remote	Ernakulam		32	Remote	Shillong
11	Remote	Kolkata		33	Remote	Srinagar
12	Remote	Mumbai		34	Remote	Jaipur
13	Remote	Mumbai		35	Remote	Kolkata-2
14	Remote	New Delhi		36	Remote	Noida
15	Remote	New Delhi		37	Remote	Chennai
16	Remote	Chennai		38	Remote	Mumbai
17	Remote	Mumbai		39	Remote	Varanasi
18	Remote	Chennai		40	Remote	Bangalore
19	Remote	Mumbai		41	Remote	Hyderabad
20	Remote	Agartala		42	Remote	Bhopal
21	Remote	Chandigarh		43	Remote	Kolkata
22	Remote	Pune		44	Remote	Lucknow
S/N	Sites	City		S/N	Sites	City
45	Remote	Ranchi		71	Remote	Bangalore

46	Remote	Pune		72	Remote	Bangalore
47	Remote	Jaipur		73	Remote	Bangalore
48	Remote	Mohali		74	Remote	Bangalore
49	Remote	Patna		75	Remote	Bangalore
50	Remote	Chennai		76	Remote	Bangalore
51	Remote	Cuddalore		77	Remote	Bangalore
52	Remote	Kohima		78	Remote	Bangalore
53	Remote	Kolkata		79	Remote	Bangalore
54	Remote	Kolkata		80	Remote	Bangalore
55	Remote	Lucknow		81	Remote	Bangalore
56	Remote	Mumbai		82	Remote	Bangalore
57	Remote	Mumbai		83	Remote	Bhopal
58	Remote	Navi Mumbai		84	Remote	Bhubaneswar
59	Remote	Pune		85	Remote	Bhubaneswar
60	Remote	Agartala		86	Remote	Chandigarh
61	Remote	Ahemdabad		87	Remote	Chennai
62	Remote	Aligarh		88	Remote	Chennai
63	Remote	Allahabad		89	Remote	Chennai
64	Remote	Bangalore		90	Remote	Chennai
65	Remote	Bangalore		91	Remote	Chennai
66	Remote	Bangalore		92	Remote	Chennai
67	Remote	Bangalore		93	Remote	Chennai
68	Remote	Bangalore		94	Remote	Chennai
69	Remote	Bangalore		95	Remote	Chennai
70	Remote	Bangalore		96	Remote	Chennai
S/N	Sites	City		S/N	Sites	City
97	Remote	Cochin		123	Remote	Hyderabad

98	Remote	Dehradun		124	Remote	Hyderabad
99	Remote	Dibrugarh		125	Remote	Imphal
100	Remote	Ernakulam		126	Remote	Imphal
101	Remote	Faridabad		127	Remote	Indore
102	Remote	Gandhinagar		128	Remote	Jaipur
103	Remote	Gangtok		129	Remote	Jaipur
104	Remote	Gurugram		130	Remote	Jaipur
105	Remote	Gurugram		131	Remote	JAMMU
106	Remote	Gurugram		132	Remote	Jamshedpur
107	Remote	Gurugram		133	Remote	Kazhakkootam
108	Remote	Gurugram		134	Remote	KOLKATA
109	Remote	Gurugram		135	Remote	Kolkata
110	Remote	Gurugram		136	Remote	Kolkata
111	Remote	Guwahati		137	Remote	Kolkata
112	Remote	Guwahati		138	Remote	Kolkata
113	Remote	Hosur		139	Remote	Purba Medinipur
114	Remote	Hyderabad		140	Remote	Kolkata
115	Remote	Hyderabad		141	Remote	Kolkata
116	Remote	Hyderabad		142	Remote	KORAPUT
117	Remote	Hyderabad		143	Remote	Lucknow
118	Remote	Hyderabad		144	Remote	Lucknow
119	Remote	Hyderabad		145	Remote	Mohali
120	Remote	Hyderabad		146	Remote	Mumbai
121	Remote	Hyderabad		147	Remote	Mumbai
122	Remote	Hyderabad		148	Remote	Mumbai
S/N	Sites	City		S/N	Sites	City
149	Remote	Mumbai		175	Remote	Vadodara

150	Remote	Mumbai		176	Remote	Mussoorie
151	Remote	Mumbai		177	Remote	Nagpur
152	Remote	Mumbai		178	Remote	Navi Mumbai
153	Remote	Mumbai		179	Remote	Navi Mumbai
154	Remote	Mumbai		180	Remote	Navi Mumbai
155	Remote	Mumbai		181	Remote	Navi Mumbai
156	Remote	Mumbai		182	Remote	Navi Mumbai
157	Remote	Mumbai		183	Remote	Navi Mumbai
158	Remote	Mumbai		184	Remote	Navi Mumbai
159	Remote	Mumbai		185	Remote	Navi Mumbai
160	Remote	Mumbai		186	Remote	Navi Mumbai
161	Remote	Mumbai		187	Remote	New Delhi
162	Remote	Mumbai		188	Remote	New Delhi
163	Remote	Mumbai		189	Remote	New Delhi
164	Remote	Mumbai		190	Remote	New Delhi
165	Remote	Mumbai		191	Remote	New Delhi
166	Remote	Mumbai		192	Remote	New Delhi
167	Remote	Mumbai		193	Remote	New Delhi
168	Remote	Mumbai		194	Remote	New Delhi
169	Remote	Mumbai		195	Remote	New Delhi
170	Remote	Mumbai		196	Remote	New Delhi
171	Remote	Mumbai		197	Remote	New Delhi
172	Remote	Mumbai		198	Remote	New Delhi
173	Remote	Mumbai		199	Remote	New Delhi
174	Remote	Mumbai		200	Remote	New Delhi
S/N	Sites	City		S/N	Sites	City
201	Remote	New Delhi		227	Remote	Pune

202	Remote	New Delhi		228	Remote	Pune
203	Remote	New Delhi		229	Remote	Pune
204	Remote	New Delhi		230	Remote	Pune
205	Remote	New Delhi		231	Remote	Pune
206	Remote	New Delhi		232	Remote	Pune
207	Remote	New Delhi		233	Remote	Raipur
208	Remote	New Delhi		234	Remote	Ranchi
209	Remote	New Delhi		235	Remote	Ranchi
210	Remote	New Delhi		236	Remote	Ranchi
211	Remote	New Delhi		237	Remote	Secunderabad
212	Remote	New Delhi		238	Remote	Shillong
213	Remote	New Delhi		239	Remote	Shillong
214	Remote	New Delhi		240	Remote	Shillong
215	Remote	New Delhi		241	Remote	Shimla
216	Remote	Nazira (Sivsagar)		242	Remote	Shimla
217	Remote	Noida		243	Remote	Tehri
218	Remote	Noida		244	Remote	Trivandrum
219	Remote	Noida		245	Remote	Tuticorin
220	Remote	Noida		246	Remote	Vasco-da-Gama
221	Remote	Noida		247	Remote	Visakhapatnam
222	Remote	Noida		248	Remote	Visakhapatnam
223	Remote	Noida		249	Remote	Visakhapatnam
224	Remote	Noida		250	Remote	Visakhapatnam
225	Remote	Panji				
226	Remote	Patna				

Section V: Technical Specifications
Technical Specification

1. Server (Category-1)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC , 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)		
Memory	16x 32GB DDR4 2933+ MHz ECC REG DIMM (Buffered). (Total 512GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64: 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	12+ no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 4GB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 6 with 12+ HDD, sequential, Block size 64KB, Queue depth 64 : 1+ GB/sec Total read speed after RAID 6 with 12+ HDD, sequential, Block size 64KB, Queue depth 64 : 2+ GB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		

Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
HW Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 8+ GB cache, battery or flash backed protection, for the 12 no:s of HDDs		
Power Supply	Redundant, maximum 1200 W		
Accessories	Rails kit for rack mounting		
General Features	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

2. Server (Category-2)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
	2A (in case bidder quote 4U server)		
Physical dimension	Maximum upto 4U		

Processor	2 Quantity (Dual Socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 18+ Cores (2.3+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 18+ cores (2.3+ GHz base frequency, Cache Size 128+ MB)		
Memory	Total 1 TB RAM, DDR4 2933+ MHz ECC REG DIMM (32 no:s x 32G OR 16 no:s x 64G)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	Storage in 4U server : 60 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 6 with 60 HDD, sequential, Block size 64KB, Queue depth 64: 5+ GB/sec Total read speed after RAID 6 with 60 HDD, sequential, Block size 64KB, Queue depth 64: 20+ GB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 8+ GB cache, battery or flash backed protection, for the 60 no:s of HDDs, where all available HDDs in the server should be configurable under a single virtual partition with RAID 5,6,50,60		

Power Supply	Redundant, maximum 1200 W		
Accessories	Accessories: Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
	2B OR (in case bidder quote server with single DAS)		
Physical dimension	Maximum upto 6U		
Processor	2 Quantity (Dual Socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ Cores (2.1+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.1+ GHz base frequency, Cache Size 128+ MB)		
Memory	Total 1 TB RAM, DDR4 2933+ MHz ECC REG DIMM (32 no:s x 32G OR 16 no:s x 64G)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		

Storage	<p>84 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours)</p> <p>Note: DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. DAS and Server should be from same OEM.</p> <p>Total write speed after RAID 6 with 80 HDD, sequential, Block size 64KB, Queue depth 64: 6+ GB/sec Total read speed after RAID 6 with 80 HDD, sequential, Block size 64KB, Queue depth 64: 25+ GB/sec</p>		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 8+ GB cache, battery or flash backed protection, for the 80 no:s of HDDs		
Power Supply	Redundant, 1200 W or above		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

3. Server (Category-3)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)		
Memory	Memory: 16x 32GB DDR4 2933MHz ECC REG DIMM (Total 512GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	4+ no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 6 with 4+ HDD, sequential, Block size 64KB, Queue depth 64: 250+ MB/sec Total read speed after RAID 6 with 4+ HDD, sequential, Block size 64KB, Queue depth 64: 700+ MB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		

Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 4+ no:s of HDDs		
Cache Drive Type	Enterprise NVMe drive for caching: Capacity: 3.2 TB ,PCI Express Gen4 x 8, NVMe Sequential read 6,200 MB/s ,Sequential write 2,600 MB/s (Sequential and Random performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS ,Random write (4K) Up to 180K IOPS Latency, read/write 120/20 μs (4KB transfer size with queue depth 1) Endurance 5 DWPD		
Power supply	Redundant, maximum 800 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

4. Server (Category-4)

Description	Specification	Marked/ Highlighted Reference Specification with reference page no.	Cross of with	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable			
Processor	Intel Xeon scalable series, 12 core processor (2.9+ GHz base frequency, Cache Size 24.75+ MB) OR AMD EPYC 7272, 12 core processor (2.9+ GHz base frequency, Cache Size 64 MB)			

Memory	8 no:s x 16GB DDR4 2933MHz ECC REG DIMM (Total 128GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	2 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 100+ MB/sec Total read speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 300+ MB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	* Baseboard management console with dedicated RJ45 interface , (IPMI)		
HW Raid controller	* HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 2+ no:s of HDDs		
Cache Drive Type	* Enterprise NVMe drive for caching: Capacity: 3.2 TB ,PCI Express Gen4 x 8, NVMe Sequential read 6,200 MB/s ,Sequential write 2,600 MB/s (Sequential and Random performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS ,Random write (4K) Up to 180K IOPS Latency, read/write 120/20 μ s (4KB transfer size with queue depth 1) Endurance 5 DWPD		
Power supply	Redundant, maximum 800 W		
Accessories	Rails kit for rack mounting		
	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		

General Features for Server	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

5. Server (Category-5)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	2 Quantity (Dual socket) x Intel Xeon 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR 2 Quantity (Dual socket) x AMD EPYC 7252, 8 core processor (3.1+ GHz base frequency, Cache Size 64+ MB)		
Memory	2 no:s x 16GB DDR4 2933MHz ECC REG DIMM (Total 32GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		

Storage	2 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 100+ MB/sec Total read speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 300+ MB/sec		
Interface (NIC)	2x 1G, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers) , 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 2+ no:s of HDDs		
Power Supply	Redundant, maximum 800 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

6. Server (Category-6)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	1 Quantity x Intel Xeon 8 core processor (2.7+ GHz base frequency, Cache Size 20+ MB) OR 1 Quantity x AMD EPYC, 8 core processor (2.7+ GHz base frequency, Cache Size 32 MB)		
Memory	2 no:s x 8GB DDR4 2933MHz ECC REG DIMM (Total 16 GB)		
Storage	2 x 8+ TB Enterprise Drives (Each HDD spec: SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 100+ MB/sec Total read speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 200+ MB/sec		
Interface (NIC)	2x 1G, copper + 2 x1G Fiber SFP (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	RAID Support : System BIOS should support for RAID 0,1 (Software RAID or HW raid)		
Power Supply	Redundant, Maximum 500 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		

	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

7. Server (Category-7)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 18+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 18+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)		
Memory	8 no:s x 32GB DDR4 2933MHz ECC REG DIMM (Total 256GB)		
Boot Storage subsystem	with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	16 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 6 with 16+ HDD, sequential, Block size 64KB, Queue depth 64: 1.5+ GB/sec Total read speed after RAID 6 with 16+ HDD, sequential, Block size 64KB, Queue depth 64: 3+ GB/sec		

Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers),		
Interface (NIC)	10G ports should be fully populated with required LR / SR Transceivers as per site requirement (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 16+ no:s of HDDs		
Power Supply	Redundant ,Maximum 1000 W		
Accessories	Accessories: Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

8. Server (Category-9)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	4U to 6U Rack Mountable		

Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)		
Memory	16 no:s x 32GB DDR4 2933+MHz ECC REG DIMM (Total 512GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	* 60 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Note: Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. DAS and Server should be from same OEM. Total write speed after RAID 6 with 60+ HDD, sequential, Block size 64KB, Queue depth 64: 6+ GB/sec Total read speed after RAID 6 with 60+ HDD, sequential, Block size 64KB, Queue depth 64: 20+ GB/sec		
Interface (NIC)	2x 1G Copper, 4x10G Fiber SFP+ (connectivity support for copper/fiber transceivers)		
Interface (NIC)	10G ports should be fully populated with required LR / SR Transceivers as per site requirement (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		

Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 8+ GB cache , battery or flash backed protection, for the 60+ no:s of HDDs		
Power Supply	Redundant, Maximum 1000 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

9. Server (Category-10)

Description	Specification	Marked/ Highlighted Reference Specification with reference page no.	Cross of with	Compliance (Yes/No)
Physical dimension	4U to 6U Rack Mountable			
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)			
Memory	32 no:s x 32GB DDR4 2933+MHz ECC REG DIMM (Total 1TB)			

Boot Storage subsystem	<p>Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD</p> <p>Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec</p> <p>Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec</p>		
Storage	<p>Storage in 4U Server: 60 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours)</p> <p>Total write speed after RAID 6 with 60+ HDD, sequential, Block size 64KB, Queue depth 64: 5+ GB/sec</p> <p>Total read speed after RAID 6 with 60+ HDD, sequential, Block size 64KB, Queue depth 64: 20+ GB/sec</p> <p>Note: Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. DAS and Server should be from same OEM.</p>		
Interface (NIC)	NIC: 2x 1G Copper, 8x10G Fiber SFP+ (connectivity support for copper/fiber transceivers)		
Interface (NIC)	10G ports should be fully populated with required LR / SR Transceivers as per site requirement (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 8+ GB cache, battery or flash backed protection, for the 60+ no:s of HDDs		
Power supply	Redundant, Maximum 1000 W		
Accessories	Accessories: Rails kit for rack mounting		
	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		

General Features for Server	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

10. Server (Category-11)

Description	Specification	Marked/ Highlighted Reference Specification with reference page no.	Cross of with	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable			
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen Epyc , 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)			
Memory	8x 32GB DDR4 2933MHz ECC REG DIMM (Total 256GB)			
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec			
Storage	Storage: 8 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours)			

	Total write speed after RAID 6 with 8+ HDD, sequential, Block size 64KB, Queue depth 64: 800+ MB/sec Total read speed after RAID 6 with 8+ HDD, sequential, Block size 64KB, Queue depth 64: 1.5+GB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers)		
Interface (NIC)	10G ports should be fully populated with required LR / SR Transceivers as per site requirement (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 8+ no:s of HDDs		
Cache Drive Type	Enterprise NVMe drive for caching: Capacity: 3.2 TB ,PCI Express Gen4 x 8, NVMe Sequential read 6,200 MB/s ,Sequential write 2,600 MB/s (Sequential and Random performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS ,Random write (4K) Up to 180K IOPS Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 5 DWPD		
Power Supply	Redundant, Maximum 800 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
	10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Feature Support	All the features mentioned above should be available from day one		

11. Server (Category-13)

Description	Specification	Marked/ Highlighted Reference Specification with reference page no.	Cross of with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable			
Processor	* Processor: 2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)			
Memory	8x 32GB DDR4 2933MHz ECC REG DIMM (Total 256GB)			
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec			
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make), 2 no:s x dual 100G QSFP28 , PCIe 4.0 (NIC: Dual port 100G. Mellanox MCX516A-CDAT ConnectX-5 Ex / Intel E810-2CQDA2)			
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)			
Power Supply	Redundant, Maximum 1200 W			
Accessories	Rails kit for rack mounting			
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu			
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization			

	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

12. Server (Category-14)

Description	Specification	Marked/ Highlighted Reference Specification with reference page no.	Cross of with	Compliance (Yes/No)
Physical dimension	1U Rack Mountable			
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)			
Memory	8x 32GB DDR4 2933MHz ECC REG DIMM (Total 256GB)			
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec			

Storage	2 no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 100+ MB/sec Total read speed after RAID 1 with 2+ HDD, sequential, Block size 64KB, Queue depth 64: 300+ MB/sec		
Interface (NIC)	NIC: 2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers) , 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 2+ no:s of HDDs		
Cache Drive	* Enterprise NVMe drive for caching: Capacity:3.2 TB ,PCI Express Gen4 x 8, NVMe Sequential read 6,200 MB/s ,Sequential write 2,600 MB/s (Sequential and Random performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS ,Random write (4K) Up to 180K IOPS Latency, read/write 120/20 μ s (4KB transfer size with queue depth 1) Endurance 5 DWPD		
Power Supply	* Redundant , Maximum 800 W		
Accessories	* Accessories: Rails kit for rack mounting		
General Features for Servers	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

13. Server (Category-16)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Physical dimension	Maximum upto 2U Rack Mountable		
Processor	2 Quantity (Dual socket) x Intel Xeon Gold scalable series 2nd / 3rd Gen, 24+ cores (2.8+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD 2nd / 3rd Gen EPYC, 24+ cores (2.8+ GHz base frequency, Cache Size 128+ MB)		
Memory	16x 32GB DDR4 2933MHz ECC REG DIMM (Total 512GB)		
Boot Storage subsystem	Boot Storage subsystem with Redundant HW RAID 1 having 2 no:s x Enterprise SAS SSD, Each SSD spec: 480GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec		
Storage	12+ no:s x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 4GB Cache, 3.5", MTBF = 8+ Lakhs hours) Total write speed after RAID 6 with 12+ HDD, sequential, Block size 64KB, Queue depth 64 : 1+ GB/sec Total read speed after RAID 6 with 12+ HDD, sequential, Block size 64KB, Queue depth 64 : 2+ GB/sec		
Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers) , 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
GPU Card	2 x NVIDIA-H100 (SXM) GPU cards with CUDA support		

Baseboard management	Offline Management: Baseboard management console = 1		
Raid controller	HW Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 2+ GB cache, battery or flash backed protection, for the 12+ no:s of HDDs		
Cache Drive	Enterprise NVMe drive for caching: Capacity: 3.2 TB ,PCI Express Gen4 x 8, NVMe Sequential read 6,200 MB/s ,Sequential write 2,600 MB/s (Sequential and Random performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS ,Random write (4K) Up to 180K IOPS Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 5 DWPD		
Power Supply	Redundant , Maximum 1200 W		
Accessories	Rails kit for rack mounting		
General Features for Server	Certification/Compliance (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu		
	Certification/Compliance (Virtualization/Cloud Platform): VM Ware, Red Hat Virtualization		
	Power Supply Efficiency: Platinum		
	For the Boot Storage (SSD) and Storage (HDD) Drives : Sanitize Instant Erase , Self-Encrypting (SED-FIPS Certified)		
Feature Support	All the features mentioned above should be available from day one		

Note: + considered as or Higher, mentioned wherever in specifications of servers from S.N. 1 to 13

Management & Security Features for all the server mentioned from S.N. 1 to 13

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
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, Real-time Health logging and telemetry streaming, power management, storage management including raid configuration, virtual media access ,Secure component verification and alerting ,Secure management with configuration of https, LDAP/radius, NTP for time sync, SNMP,API based management support, along with support of Redfish, IPMI etc.,HTML 5 based virtual console, Remote Firmware, bios, driver update, Dedicate Ethernet port, and OOB baseboard management controller , Agent free, browser-based and command-line interface for managing and monitoring the server hardware.		

Management Features-2	<p>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 System to enable users to filter and sort systems based on user assigned attributes, Hardware Profile based deployment to multiple Servers simultaneously, Policy template for deployment of single policy to multiple Servers simultaneously, 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, Solution should be open and programmable providing Rest API, SDK for programming languages like Python , power shell scripts etc., Should have customizable dashboard to show overall faults/health/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. the user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc.), Self-service portal deployment for automated provisioning, Real-time out-of-band hardware performance monitoring & alerting</p>		
Security Features-1	<p>Secure Boot(Firmware and Bios Level Security), Provision to lock the system on breach, Hardware root of trust/Dual Root of Trust, Server should provide policy based security, Server should provide server intrusion detection,, "Malicious Code Free design" (to be certified by OEM).</p>		
Security Features-2	<p>Provision for Cryptographic firmware updates, Capability to stop execution of Application/Hypervisor/ Operating System on predefined security breach, Secure /Automatic BIOS recovery, Network Card secure firmware boot, in case of any security breach system should provide the lock down feature. Support for TPM 2.0</p>		

General Note	Bidder shall supply required quantity of fiber patch chords (Single mode/ Multimode), patch chord as per site requirements. All accessories for successful installation in rack should be supplied by Bidder. Supplied equipment must be mountable on 19-inch rack. The device should have front to back airflow with efficient cooling mechanism. All the features mentioned above should be available from day one		
Additional SFP requirements	Bidder shall additionally supply 10% extra SFPs compatible with servers.		

Networking Specifications of DC and DR

It may be noted that all the OEMs of Networking Devices should provide their respective Intent-Based Networking Software License.

14. DC Spine Switch

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Core Switch	Chassis Based		
No. of Interface Slots	8 or higher		
No. of MPU/SUP/RE/ Fabric Slots	2 or higher		
No. of Routing engines/ Supervisor Modules	2 or higher		
No. of FAN Tray	2 or higher		
Support for 100G QSFP28 Port	Yes		
Number of 100G QSFP28 Port	120 or higher		
Switching Capacity (Gbps)	48000 or higher		
a. Advance Layer-3 Protocol	a. EVPN-VXLANESI-LAG(No proprietary solutions are to be deployed)		
b. Security Feature	b. Port,VLAN&RoutedACL,64K ACL Entries /extended ACL /terms ,GRE (Must Support 1000 or Higher GRE Tunnels & 1000 VXLAN Tunnels)		
c. Management Protocol	c. Role Based CLI,SNMPv1/v2/v3,Open stack, Python, XML, SSH, Streaming Telemetry, gRPC, Netconf, ZTP		

d. QoS	d. Virtual output Queue VoQ)/Egress QoS, WRED,LLQ,PTP,12GB Buffer per line card, 802.1Qbb,8 queues/port, WRR		
Management solution	Datacentre Fabric Management solution that supports unified management to fabric including spine and leaf switches with Zero Touch provisioning of all DC Fabric Nodes.		
	Fabric Management solutions should provide Advanced telemetry that can collect streaming telemetry data from switches and monitor and get alerts on data transfers across a fabric.		
	Management solution should support integrated and customizable visualizations for path analysis, heat maps and bandwidth visualization		
	Should support creation of Service Level Agreements in one central location and alert any time there is a deviation from defined properties.		
	Should have ability to check the compliance of devices and services across the entire fabric.		
	Hardware and software (Compute & Storage) required for Fabric Manager & Element Managers shall be provided from day 1		
Other Features	Should support 900K IPv4 Routes,900K IPv6 Routes,128K IPv4 Multicast Routes &128K IPv6 Multicast Routes.		
Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
Redundant FAN	Redundant FAN for fully loaded chassis from day 1		
Feature Support	All the features mentioned above should be available from day one		

15. DC Leaf Switch

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
No of SFP/ SFP+ Ports	Minimum 48 Nos		
Type of SFP Port	10G		
Support for 100GQ SFP+ Port (Uplink)	Yes		
No .of 100G QSFP+ Port	4 or higher		
Switching Capacity (Non-Blocking) (Gbps)	2560 or higher		
a. Advance Layer-3 Protocol	a. EVPN-VXLANESI-LAG(No proprietary solutions are to be deployed)		
b. Security Feature	b. Port, VLAN & Routed ACL,1500 Ingress&1500 Egress ACL Entries, 802.1x		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3,Open stack, Python, XML, SSH, Streaming Telemetry, gRPC, Netconf, ZTP		
d. QoS	d. WRED,SPQ,SDWRR/WRR,32MBBuffer,802.1Qbb,802.1Qaz,8q ueues/port, Remarking of bridged packets		
Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
Redundant FAN	Redundant FAN for complete Chassis from day 1		
Feature Support	All the leaf switches (planned for DC & DR) should have license to integrate with Spine switch and Fabric Manager. All the features mentioned above should be available from day one		

16. DC OOB Core Switch

Description	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
No of 10G SFP/SFP+ Ports	Minimum 48 Nos		
Type of SFP Port	10G		
Support for 100GQSFP+ Port (Uplink)	Yes		
No .of 100G QSFP+ Port	6 or higher		
Switching Capacity (Non-Blocking) (Gbps)	2560 or higher		
a. Advance Layer-3 Protocol	a. EVPN-VXLANESI-LAG(No proprietary solutions are to be deployed))		
b. Security Feature	b. Port, VLAN & Routed ACL,1500 Ingress & 1500 Egress ACL Entries, 802.1x		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3,Openstack,Python,XML,SSH, Streaming Telemetry, gRPC, Netconf, ZTP		
d.QoS	d. WRED,SPQ, SDWRR / WRR, 32MB Buffer,802.1Qbb, 802.1Qaz, 8queues /port, Remarking of bridged packets		
Stacking	Should be supplied on day 1 with stacking/Inter-connect cable of 5 meter length		
Redundant Power Supply	Internal Redundant Power Supply fully loaded from day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		

Feature Support	All the features mentioned above should be available from day one		
-----------------	---	--	--

17. DC OOB Access Switch

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Number of 10/100/1000Base-T Ports	48 or higher		
Number of 10G SFP+ Port(Uplink)	4 or higher		
Number of 40GQSFP+ Port (Uplink)	2 or higher		
Switching Capacity / Forwarding Bandwidth (Non-Blocking) (Gbps)	336 or higher		
Number of VLAN Supported	4096		
Layer2 Protocols	802.1QVLAN,LAG,LACP,STP,MSTP,RSTP,IEEE802.3x,VLAN		
Basic Layer-3 Protocol from day1	Static Routing, PBR		
Advance Layer-3Protocol support	OSPFv2,OSPFv3,PIM-SM,PIM-SSM		
Premium Layer-3 Protocol support	VRF Lite, VRF,PIM-DM,VRRP		

Security Feature	RA Guard or equivalent, DHCP Snooping, Dynamic ARP Inspection(or similar security feature which validates ARP packets and prevents attacks such as MITM/(Control Plane Policing (CoPP), ARP cache poisoning		
Management Protocol	GUI,CLI,Telnet,TFTP,,SNMPv1,SNMPv2/V2C,SNMPv3,NTP, RMON,SSHv2, Single IP Management		
QoS	802.1p,SP,Queues per port, WRED /WTD, Sflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing		
Stacking	Should be supplied on day1with stacking/Inter-connect cable of 5 meter length		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

18. Layer 3 Access Switch (48 Ports)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Number of 10/100/1000Base-T Ports	48 or higher		
Number of 10G SFP+ Port(Uplink)	4 or higher		

Number of 40GQSFP+ Port (Uplink)	2 or higher		
Switching Capacity / Forwarding Bandwidth (Non-Blocking) (Gbps)	336 or higher		
Number of VLAN Supported	4096		
Layer2 Protocols	802.1QVLAN,LAG,LACP,STP,MSTP,RSTP,IEEE802.3x,VLAN		
Basic Layer-3 Protocol from day1	Static Routing, PBR		
Advance Layer-3 Protocol support	OSPFv2,OSPFv3,PIM-SM,PIM-SSM		
Premium Layer-3 Protocol support	VRF Lite, VRF,PIM-DM,VRRP		
Security Feature	RA Guard or equivalent, DHCP Snooping, Dynamic ARP Inspection(or similar security feature which validates ARP packets and prevents attacks such as MITM/(Control Plane Policing (CoPP), ARP cache poisoning		
Management Protocol	GUI,CLI,Telnet,TFTP,,SNMPv1,SNMPv2/V2C,SNMPv3,NTP, RMON,SSHv2, Single IP Management		
QoS	802.1p,SP,Queues per port, WRED /WTD, Sflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing		
Stacking	Should be supplied on day1 with stacking/Inter-connect cable of 5 meter length		

Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

19. DR CE Router/ Internal WAN Router

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Router	WAN		
Routing Engine	The Router should be populated with redundant Routing Card/Engines		
Aggregated Throughput (Gbps)	2400 Or higher		
Port population	Should be supplied with 12 numbers of 100G QSFP28 ports		
Number of Routes	Should support 1MIPv4 & 900K IPv6 Routes		
Routing Protocols from day-1	OSPF ,BGP MPLS, EVPN-MPLS, Segment Routing, Multicasting-MVPN, MOFRR, GMPS,,RSVP-TE, LDP, BGP-LU-SR-TE		
Network Management Protocols	Role based cli, config rollback, python scripts, rest API, netconf, xml, schema, secure boot/signed image verification, secure copy		
IPsec Throughput (Mbps)	Any applicable numeric value		

Security Protocol	radius,802.1x,tacacs,stateless ACL ,dynamic ACL ,rule propagation via BGP, control plane dos,		
QoS	Support Class-Based Weighted Fair Queuing (CBWFQ) or Weighted round robin queuing, WRED, Hierarchical QoS for Traffic Management, inspections.		
IPv6 Ready	IPv6:OSPF v3 and static routers ipv6 Routing IPv6 Multicast IPv6 QoS, IPv6 VPN over MPLS		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

20. DC Border Leaf Switch

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type Of Core Switch	Chassis Based, Non-Chassis Based		
Support for 100G QSFP+ Port	Yes		

No. of Ports	Should have minimum 24Nos of 100G QSFP28 Ports		
Switching Capacity (Gbps)	4800 Or higher		
a. Advance Layer-3 Protocol	a. MPLS EVPN-VXLAN VRF (No proprietary solutions are to be deployed))		
b. Security Feature	b. Port, VLAN, ACL, Routed ACL		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3,Openstack,Python,XML,SSH, Streaming Telemetry, gRPC, Netconf ,ZTP		
d. QoS	d. WRED,SPQ,SDWRR/WRR, 32MB Buffer, 802.1Qbb, 802.1Qaz, 8 queues / port, Remarking of bridged packets		
Other features	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 1M IPv4 Routes,1M IPv6 Routes, 64K Multicast Route		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	Switch should have license to integrate with Spine switch and Fabric Manager. All the features mentioned above should be available from day one		

21. DC Internet Router

Description	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Router	WAN		
No. of 10G SFP+ ports (Fiber /Copper)	8 Or higher		
Port population	Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 10/100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to additional 2 X 40G		
Switching Capacity (Non-Blocking) (Gbps)	256 or higher		
Number of Routes	Should support 1.5M IPv4 & 900K IPv6 Routes		
Routing Protocols	OSPF, BGP, MPLS, EVPN-MPLS ,Segment Routing, Multicasting MVPN, MOFRR, GMPLS, RSVP-TE ,LDP, BGP-LU, SR-TE		
Network Management Protocols	Role based CLI, Config rollback, python scripts, rest API , Netconf, xml schema, secure boot/signed image verification, secure copy		
Security Protocol	Schema, secure boot/signed image verification, secure copy		
QoS	Support Class-Based Weighted Fair Queuing (CBWFQ) or Weighted round robin queuing, WRED, Hierarchical QoS for Traffic Management, inspections.		
IPv6 Ready	IPv6:OSPFv3 and static routers IPv6 RoutingIPv6 Multicast IPv6QoS IPv6 VPN over MPLS		

Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

22. DC Interconnect Switch - Type 1

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Core Switch	Chassis Based, Non-Chassis Based		
Support for 100G QSFP+ Port	Yes		
No. of Ports	Should have minimum 8 Nos of 10G and 16 Nos of 100G QSFP28 Ports		
Switching Capacity (Gbps)	3360 Or higher		
a. Layer 2 Protocols	a. VLAN, LAG, LACP, STP, MSTP, RSTP, IEEE 802.3x		
b. Basic & Advance Layer-3 Protocol	b. EVPN-VXLANESI-LAG (No proprietary solutions are to be deployed))), OSPFv2, OSPFv3,PBR, BGP, BGP4 , IS-IS-PIM-SSM, PIM-DM		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3, Open stack, Python, XML,SSH, Streaming Telemetry, gRPC, Netconf, ZTP		

d. QoS	d. WRED,SPQ,SDWRR/WRR,32MB Buffer, 802.1Qbb, 802.1Qaz, 8queues /port, Remarking of bridged packets		
Security Feature	VLAN & Routed ACL,1500 Ingress &1500 Egress ACL Entries, 802.1x , RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping		
Stacking	Should be supplied on day1with stacking/Inter-connect cable of 5 meter length		
Other features	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an on-blocking fabric		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

23. DC Interconnect Switch - Type 2

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Core Switch	Chassis Based, Non-Chassis Based		
Support for 10 SFP & 100G QSFP+ Port	Yes		
No. of Ports	Should have minimum 16Nos of 10G and 8 Nos 100G QSFP28 Ports		

Switching Capacity(Gbps)	1920 Or higher		
a. Layer 2 Protocols	a. 802.1Q VLAN, LAG, LACP, STP, MSTP, RSTP, VxLAN, IEEE 802.3x,VLAN		
b. Basic & Advance Layer-3 Protocol	b. EVPN-VXLANESI-LAG(No proprietary solutions are to be deployed))), Static routing, RIPv1, RIPv2, BGP, OSPFv2, OSPFv3, PBR		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3,Openstack,Python,XML,SSH, Streaming Telemetry, gRPC, Netconf, ZTP		
d. QoS	d. WRED,SPQ, SDWRR/ WRR,32MB Buffer, 802.1Qbb ,802.1Qaz, 8queues /port, Remarking of bridged packets		
Security Feature	VLAN & Routed ACL,1500 Ingress & 1500 Egress ACL Entries, 802.1x , RADIUS/TACACS, Port Security or equivalent ,BPDU Guard, IGMP snooping		
Stacking	Should be supplied on day1with stacking /Inter-connect cable of 5 meter length		
Other features	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an on-blocking fabric		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

24. DC WAN Switch

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Core Switch	Chassis Based, Non-Chassis Based		
No. of FAN Tray	2 Or higher		
Support for 100G QSFP+ Port	Yes		
No. of Slots	Should be populated with 4x1GBase-LX, 4x10/100/1000 Base-T, 4x10G Base-LR and 4 x 10GBase-SR transceivers. Also should have minimum 16 Nos of 100G QSFP28 Ports and populated with 8 x 100G Transceivers (LR/SR will be decided as per TSP MUX)		
Switching Capacity (Gbps)	4800 Or higher		
a. Advance Layer-3 Protocol	a. EVPN-VXLANESI-LAG(No proprietary solutions are to be deployed))		
b. Security Feature	b. Port, VLAN & Routed ACL, 1500 Ingress & 1500 Egress ACL Entries, 802.1x		
c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3, Open stack, Python, XML, SSH, Streaming Telemetry, gRPC, Netconf, ZTP		
d. QoS	d. WRED, SPQ, SDWRR/ WRR, 32MB Buffer, 802.1Qbb, 802.1Qaz, 8 queues /port, Remarking of bridged packets		
Other features	Switch should support all functions required to operate as a WAN Switch acting as interface between Service Provider Links and WAN Router		
Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
Redundant FAN	Redundant FAN for fully loaded chassis from day 1		

Feature Support	All the features mentioned above should be available from day one		
-----------------	---	--	--

25. SFP Transceiver-10GBase-SR (For Networking Equipment)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no	Compliance (Yes/No)
Type of Transceiver	SFP+10GBase-SR Transceivers		
SFP Mode	Multi		
Compatibility with OEMs Products	all		
Fibre Cable Type	MMF		
Maximum Data Rate	10 Gbps		

26 SFP Transceiver -10GBase-LR (For Networking Equipment)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no	Compliance (Yes/No)
Type of Transceiver	SFP+10GBase-LR Transceivers		
SFP Mode	Single		
Compatibility with OEMs Products	all		
Fibre Cable Type	SMF		
Maximum Data Rate	10 Gbps		

27. QSFP+28 Transceiver-100 GBase-SR4 (For Networking Equipment)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no	Compliance (Yes/No)
Type of Transceiver	QSFP 28 - 100GBase-SRTransceivers		
SFP Mode	Multi		
Compatibility with OEMs Products	All		
Fibre Cable Type	MMF		
Maximum Data Rate	100 Gbps		

28. QSFP+28 Transceiver-100GBase-LR4 (For Networking Equipment)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no	Compliance (Yes/No)
Type of Transceiver	QSFP 28 -100 GBase-LR4 Transceivers		
SFP Mode	Single		
Compatibility with OEMs Products	all		
Fibre Cable Type	SMF		
Maximum Data Rate	100Gbps		

29. Remote Router/ Firewall – 2Gbps (In Remote Sites)

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type of Router	WAN		
Port population	Should be supplied on day 1 with 12 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-LX Single Mode SFP transceivers and 2 x 10G Base SR Transceivers		
Routing Protocols from day-1	ospf,bgp,mpls,rsvp,ldp,l3vpn,l2vpn,mvpn,mpls-frr,mpls-te		
Network Management Protocols	Role based CLI, Web-UI, Config roll back, Python Scripts, Rest-API, ZTP, TWAMP		
IPsec Throughput	2Gbps (Packet size:1400bytes)		
IPsec Encryption	site-to-site, hub and spoke, advpn or equivalent, aes-gcm, sha-384,hmac-sha-256		
Security Protocol	Stateful firewall, distributed dos, ipv6 nat,802.1x		
QoS:	Support Class-Based Weighted Fair Queuing (CBWFQ) or Weighted round robin queuing, WRED, Hierarchical QoS/8 queues per port for Traffic Management, inspections, QoS classification with TCP Application traffic.		
IPv6 Ready	IPv6:OSPFv3 and static router sipv6 Routing IPv6 Multicast IPv6 QoS IPv6 VPN over MPLS/ GRE		
Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
Redundant FAN	Redundant/Multiple FAN fully loaded from day 1		
Feature Support	All the features mentioned above should be available from day one		

30. Internet Firewall with IPS

S.No	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Hardware Architecture		
1.1	The appliance-based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance		
1.2	Firewall appliance should be supplied with at least 8 x 1GE RJ-45 interfaces and 10 x 10G SFP+ SR interfaces slot, 4x 100GE QSFP28/40GE QSFP slot. (8x10G SFP+ SR and 4x40GE QSFP+ SR transceiver included from day one)		
1.3	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system		
1.4	Firewall & IPsec should be ICSA Lab certified		
1.5	All the features asked should support from day one and should be from same OEM. Any open source and third party solution is not accepted		
2	Performance & Scalability		
2.1	Firewall should support at least 100 Gbps of throughput on 64 byte packets. The firewall performance should not degrade while IPv6 is enabled in future		
2.2	Should support at least 15 Gbps of Mix / production performance with firewall, IPS, AVC & Anti-malware combined		
2.3	Firewall should support at least 20 Million concurrent sessions and scalable to 30 Million		
2.4	Firewall should support at least 1 Million sessions per second and scalable to 2 Million		
2.5	Firewall should support at least 1000 VLANs		
2.6	Firewall should support at least 50 Gbps of IPSEC VPN throughput		
3	Firewall Features		
3.1	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP		

3.2	Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously		
3.3	Firewall should support operating in routed & transparent mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 10 virtual firewall license to be provided from day 1		
3.4	Should support Static, RIP, OSPF, OSPFv3 and BGP		
3.5	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pa		
3.6	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality		
3.7	Firewall solution should support DNS64 & DHCPv6		
3.8	Firewall should support Multicast protocols like IGMP, PIM, etc.		
3.9	Should support security policies based on group names in source or destination fields or both		
3.10	Should support capability to limit bandwidth on basis of apps/groups, Networks / Geo, Ports, etc.		
4	High-Availability Features		
4.1	Firewall should support Active/Standby and Active/Active failover		
4.2	Firewall should support ether channel or equivalent functionality for the failover control and providing additional level of redundancy		
4.3	Firewall should support redundant interfaces to provide interface level redundancy before device failover		
4.4	Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.		
4.5	Firewall should have integrated redundant power supply		
5	Next Generation IPS		
5.1	Should have the capability to inspect SSL traffic. The SSL inspection throughput should not be less than 15 Gbps		
5.2	Should be capable of tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
5.3	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		

5.4	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
5.5	Should be capable of detecting and blocking IPv6 attacks.		
5.6	Should support more than 10,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
5.7	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.		
5.8	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
5.9	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
5.10	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.		
6	Antivirus		
6.1	Firewall should have integrated Antivirus solution if not please quote separate appliance		
6.2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:		
6.3	a) HTTP, HTTPS		
6.4	b) SMTP, SMTPS		
6.5	c) POP3, POP3S		
6.6	d) IMAP, IMAPS		
6.7	e) FTP, FTPS		
6.8	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
8	Management		

8.1	The management must be accessible via a web-based interface and ideally with no need for additional client software`		
8.3	The management solution must provide a highly customizable dashboard.		
8.4	The management solution must be capable of role-based administration		
9	Reporting		
9.1	Following are the minimum technical requirements for the appliance/Virtual appliance used for log management:		
9.2	support 8 Tera bytes of storage for log storage		
9.3	The solution shall provide a unified dashboard to monitor the real-time events/ logs of all managed devices.		
9.4	The solution shall allow monitoring of activities such as the resources, applications, and services accessed in the network.		
9.5	The solution shall allow filtering of logs based on various parameters like user, source & destination IP address, source & destination ports, services etc.		
9.6	The solution shall allow generation of reports with following information : Application Traffic Intrusions and attacks observed Top Source and destinations Top Applications Traffic statistics.		
9.7	Should support multiple Report format like PDF, HTML, CSV and XML		
9.8	Should support Run reports on-demand or on a schedule with automated email notifications, uploads and an easy to manage calendar view.		

31. DC Internal Firewall

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type	NGFW Or higher		
Features	Layer 3-Layer 4,NAT, Next Generation Intrusion Prevention System (IPS)		
Traffic handled	TCP,UDP,HTTP/TCP,TCP/UDP		
Throughput (Real World/Prod Performance) (All Features enabled)(Mbps)	234000 or higher		
Concurrent Session/Concurrent Connection	55M Or higher		
New session/Connection per second	500K Or higher		
IPsec Throughput (Mbps)	150 Gbps or better (Packet size:1400Bytes)		
Port population	Should be supplied on day1 with 8x10GBase-SR Transceivers and 12 x100G Base-SR4 Transceivers		
Power Supplies	Dual Or higher		
Details of the Firewall Policies for the Firewall provided with the License	Application Visibility License, IPS License		
Tunnels	IPSEC VPN (Site to site), Hub and Spoke , Group VPN / GDOI		
Internet Key Exchange	IKEv1, IKEv2		

Security mechanism	State full signatures, protocol anomaly detection		
NG IPS Signature supported	5000 or Higher		
Number of IPsec VPN Peers Supported (Site to Site)	10000 Or higher. Licenses to be included from day one		
Certification	Common Criteria/Indian Common Criteria Certification Scheme(IC3S)		
Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
Redundant FAN	Redundant FAN for fully loaded chassis from day 1		
Feature Support	All the features asked should be available from day one and should be from same OEM. Any open source and third party solution is not accepted		

32. DC Solution/Application Firewall

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type	NG FW Or higher		
Features	Layer3-Layer4,NAT,ApplicationVisibility and Control(AVC),Next Generation Intrusion Prevention System (IPS)		
Traffic handled	TCP,UDP,HTTP/TCP		
Packet Size	1024B		

Throughput (Real World/Prod Performance) (All Features enabled)(Mbps)	60000 or higher		
IPsec Throughput	50 Gbps		
Concurrent Session/Concurrent Connection	40M Or higher		
New session/Connection per second	380K Or higher		
Type of Interface Supported Multi-select	GE Copper, 10GSFP+, QSFP+40G, GESFF, QSFP28 100G		
Port Population	The Firewall should have minimum 16 X 10GSFP+, 3X40G QSFP and 2X100G QFSP 28. All the ports shall be fully Populated with respective Transceivers		
Details of the Firewall Policies for the Firewall provided with the License	Application Visibility License, IPS License		
Tunnels	IPSEC VPN (Site to site), Hub and Spoke , Group VPN / GDOI		
Internet Key Exchange	IKEv1, IKEv2		
Security mechanism	State-full signatures, protocol anomaly detection		
Number of IPsec VPN Peers	5000 Or higher. Licenses to be included from day one		
Supported (Site to Site)	Internal Redundant Power Supply for fully loaded chassis from day 1		
NG IPS Signature supported	5000 or higher		
Certification	Common Criteria/Indian Common Criteria Certification Scheme(IC3S)		

33. AAA (Authentication, authorization, and accounting) Server

S/N	AAA Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The AAA solution should be available as a hardware based appliance		
2	The solution must have both Radius and TACACS+ server as a built-in capability and should not have dependency on external server for AAA.		
3	AAA license should be provided to support 5000 devices from day 1 for network device administration using RADIUS and TACACS+ and scalable up to 10000 devices		
4	Solution must be provided in High Availability mode to support Active-Passive deployment.		
5	The solution should be deployed in out-of-band mode. The AAA solution should be integrated with proposed EMS to support overall required functionality .		
6	The proposed solution must provide ND (Next Day) RMA support.		
7	The proposed solution / OEM must have local in country native speaking L0 / L1 / L2 / L3 technical support centres in India.		
8	The OEM should have local in country RMA depo.		
9	The OEM must have their R&D center in India developing NAC software locally.		
10	AAA Server should provide authentication services to all the users connecting to the network and network infrastructure devices.		
11	AAA Server should support standard Radius for Authentication, Authorization and Accounting.		
12	AAA Solution should also support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices, auditing of commands executed on NEs.		
13	TACACS+ device administration should support: i. Role-based access control ii. Per Command level authorization with detailed logs for auditing		

	iii. Logging of commands executed in each user session & its availability for audit purposes and Logs should be available as per user defined period a max upto 1 year.		
14	The solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, ? (any character), * (matches any), etc and support stacking as well		
15	The proposed AAA solution must be capable of supporting 802.1X authentication and shall work with endpoint device native OS supplicant and network devices (authenticator) that are enabled for IEEE 802.1X authentication.		
16	Solution should support MAB address based authentication for unmanaged endpoints like IP phone, IP Camera, Printer, IoT.		
17	It should support Authentication by validating any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access		
18	The proposed solution should be able to integrate with industry leading Directory server like but not limited to LDAP server and Microsoft Active Directory		
19	The AAA server should support the following authentication protocols EAP-PEAP EAP-TLS EAP-MD5 PAP CHAP MS-CHAP and MS-CHAPv2		
20	Device command set authorization Network access restrictions and administrative access reporting. Restrictions such as time of day, day of week and session time limits. User and device group profiles. Should have a Web-based user interface to simplify and distribute configuration for user group profiles		
21	The AAA Server should be able to support large networked environments and support for redundant servers, remote databases, and user database backup services. Lightweight Directory Access Protocol (LDAP) authentication forwarding support for authentication of user profiles stored in directories from leading vendors		

22	Different access levels for each AAA Server administrator- and the ability to group network devices- enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a networks		
23	The AAA server should support Time Based Access		
24	The solution should be vendor agnostic and based on open standard		
25	The AAA server should support Location and device-based profiles for groups		
26	The AAA server should support Account lockout and account blacklisting		
27	The proposed AAA solution should have a built-in Profiler for network device visibility. Solution should be able to detect both new and existing endpoints and categorizes them based upon the type of endpoint (Ex: Windows, Printer, Network Device, IP Camera, Android, iPad, etc)		
28	The proposed AAA solution must support network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network		
29	The proposed AAA solution should provide support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network all within the same appliance		
30	The proposed AAA solution must support Profiling via Active and Passive collectors like DHCP, SNMP, HCP fingerprinting, HTTP-agent, NMAP, WMI, TCPIP, SMB, etc.		
31	The proposed AAA solution must provide active scanning via WMI, SSH, LDAP, SNMP and MDM Collector.		
32	The proposed AAA solution must provide flexible filtering capabilities to sort out device information based on different attributes (e.g MAC address, Manufacturer name, hostname, IP address, etc.)		
33	The proposed AAA solution should produce a real-time endpoint discovery with detailed information including which switch port the device is connected.		
34	The proposed AAA solution must provide device inventory in CSV, Tab Delimiter and PDF exportable format.		
35	The proposed AAA solution must provide capability to import device inventory via CSV and binary file.		

36	The proposed AAA solution must provide information on how many devices are not profiled, how many devices are newly seen in day/week/month, etc.		
Feature Support	All the features asked should be available from day one and should be from same OEM. Any open source and third party solution is not accepted		

34. Load balancer

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
General Specifications	All the features asked should be available from day one		
	Must support high availability		
	Must support SNMP for polling of system statistics		
	Must support SNMP Traps for key system thresholds (specify)		
	Must display a visual representation of authentication in the GUI		
	Must log all authentication events: Locally and Via syslog		
	Must support backup of the full system configuration via the GUI		
	Must support automated backup of configuration to an external location		
	Must support a local user database		
	Must have built-in tcp dump-like tool and log collecting functionality		
	Must support REST API for integration with 3rd party management and monitoring		
	Must provide detailed logs and graphs for real time and time based statistics		
	Must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.		
	Must support led warning and system log alert for failure of any of the power and CPU issues		
	The solution should support minimum 12/10 Gbps L4/L7 Throughput		
The solution should support 5 Gbps SSL Bulk Encryption Throughput			
The solution should support 15 K SSL transactions per second			

	The Appliance must support minimum 4*10/100/1000 Mbps ports, two SFP Slots and 2 * 10G SFP+ slots		
	The solution must be appliance based, rack mountable and it should be having internal redundant Power Supply from day one		
	The proposed solution should support Virtualization. Should be licensed for minimum 15 Virtual System/Virtual Domains from day one		
Load Balancing requirements	The appliance Must support layer 2 to layer 7 load balancing		
	The appliance Must support server load balancing methods		
	Must support one arm, reverse and transparent proxy mode deployment scenarios		
	Must maintain server persistency		
	Must provide application & server health checks for well-known protocols		
	Must support layer4 and layer 7 load balancing for well-known protocols		
	Must support graceful shut down of real services		
	Must support content routing		
	Must support scripting		
Link Load Balancing requirements	Must support outbound Link Load Balancing		
	Must support outbound multi-homing Link Load Balancing		
Global Server Load Balancing requirements	Must support load balancing of servers between different data centres		
	Must support dynamic proximity		
	Must support inbound Link Load Balancing		
	Must support cloud-based global server load balancing services		
	High Availability Requirements		
	Must provide comprehensive and reliable support for high availability and N+1 clustering based on Stateful session failover with Active-active & active standby unit redundancy mode.		
	Must support communication link for real-time configuration synchronization		
	Must support floating IP address and group for Stateful failover support		

	Must support built in failover decision/health check conditions		
	Must support configuration synchronization at boot time and during run time to keep consistence configuration on both units.		
SSL Offloading Requirements	Must provide secure online application delivery using hardware based high performance SSL acceleration		
	Must support certificate formats		
	Must support Certificate/Private Key backup/restore to/from local disk or remote TFTP server, and through Web UI		
	Must support self-generated CSR (Certificate Signing Request), self-signed Certificate and private key for specified host.		
	Must support customization for SSL Error pages		
	Must support HTTP to HTTPS header rewrite for enhanced application delivery support		
	Must have end to end SSL support to act as a SSL Server and/or as SSL Client		
	Must support client certificate verification, CRL's (HTTP, FTP, LDAP) and OSCP protocol		
	Must support Elliptic Curve Diffie-Helman ciphers		
	Must support TLS SNI extension		
	Must support customizable SSL/TLS versions		
	Must support SSL Forward Proxy		
Security and Application Acceleration	Must provide performance optimization using TCP connection multiplexing, TCP buffering		
	Must support IEEE 802.3ad link aggregation		
	Must provide real time Dynamic Web Content Compression to reduce server load.		
	Must provide selective compression for Text, HTML, XML, Java Scripts Mime types and pictures		
	Must provide Advanced high performance memory/packet based Web cache		
	Must provide support for customized cache rules including max object size, TTL objects, refresh time interval etc		
	Must provide detailed cache access statistics based on ip or http hosts		

	Must have security SYN flood protection		
	Must have the capability of Rate shaping & QoS Support		
	Must support Stateful firewall		
	Must support Web Application Firewall		
	Must support HTTP authentication		
	Must support IP reputation		
	Must support Geo-IP security for DDoS mitigation		
	Must support policy-based Connection limiting		

35. NDR (Network detection and response)

Sl. No	Specification Network Detection and Response (NDR)	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The solution should be on premise and should not require internet access for day to day functionality. Any required update should be supported offline.		
2	The solution should support continuous full packet capture at all sites, for intended traffic (not just malicious traffic) to enable forensic investigations and threat hunting without the need for any 3rd party solution integrations and VM/host agents		
3	The solution should natively support analysing raw network packet data, including UDP traffic, from layer 2 to layer 7 of the OSI stack for complete threat analysis. The solution should not be limited to only sampled or meta-data (e.g. IPFIX or Net Flow) analysis.		
4	The solution should provide an independent and comprehensive analysis of the attack surface by uniquely identifying and profiling endpoints (containers, virtual machines, etc.) based on behavioural fingerprints without depending on endpoint agent based solutions.		
5	The solution should be able to identify malicious activity by tracking commonality & frequency without requiring a baseline or training period.		

6	The solution should not depend exclusively on static rules such as IDS signatures, Suricata or Yara rules for threat detection. The solution instead should primarily use artificial intelligence-based approaches to detect attacks.		
7	The solution should maintain an updated 90-day profile of all devices including a summary of protocol history to aid in the discovery of low-and-slow attacks.		
8	The solution should detect threats in encrypted traffic without the need to decrypt. For example, the solution should check the commonality and frequency of TLS ciphers and destinations, without requiring support from existing network switches, endpoint agents or network proxies.		
9	The solution should have search capabilities that allow the end user to search over a minimum of 90 days of traffic history for IP addresses, domain, username, email addresses or device names. All advanced analytics capabilities should be supported for all devices with the ability to query a minimum of 90 days of history without requiring 3rd party integrations.		
10	The solution should detect threats with thin clients such as VDI instances and containers even if these do not have any logging or endpoint security deployed within.		
11	The solution should detect and respond to threats based on MITRE ATT&CK tactics and techniques.		
12	The solution should natively detect indicators of compromise and early warning signs of ransomware such as the use of doppelganger domains, inbound remote desktop, clear text passwords, unauthorized use of remote management tools, etc.		
13	The solution should natively detect living-off-the-land attacks that use tools such as PSEXEC, PowerShell, WMI, remote registry etc.		
14	The solution should have an incident management workflow component with built-in automation that automatically: <ul style="list-style-type: none"> ● Visually maps out the devices and external destinations involved in the incident ● Visually maps the relationships between the devices involved. ● Automatically generates an incident of the attack when new traffic is added. ● Provides a PDF report that can be independently shared outside the solution. 		

15	The solution should support a RESTful API and syslog forwarding to push alerts to ticketing systems and other 3rd party systems in order to assist workflow management.		
16	The solution should provide a RESTful API to allow endpoint detection & response (EDR) and security orchestration (SOAR) to implement response actions.		
17	The solution should integrate with firewalls and other network devices to enable blocking / segmentation.		
18	All required licenses for 3rd party integration should be included in the solution from day 1. Any integration that may be required in future should not be of any additional cost, for the duration of the contract		
19	The solution should support a single unified dashboard for geographically dispersed analytics engines.		
20	All licencing should be quoted along with the product to meet all the technical specifications. Any new software upgrades, features and threat detection models that come out in the future and should be available at no additional cost for the duration of the contract.		
21	The OEM must provide professional services to build custom detection models for customer's specific use cases, provide playbooks for network investigation and analysis.		
22	The OEM professional services should share methodologies for network threat hunting, should provide knowledge transfer and handover training.		
23	The solution should support identification and analysis of all devices without the need for endpoint agent installation.		
24	The solution should out of the box detect command and control to web domains that are rare in the customer environment without relying on indicators of compromise, web reputation systems or threat intelligence.		
25	The solution should out of the box detect the use of defence evasion techniques such as proxy usage to hide data exfiltration and user agent spoofing to hide the source application.		
26	The solution should out of the box detect when attack tools are shared over SMB (file share).		
27	The solution should out of the box detect indicators of compromise and early warning signs of ransomware such as the use of doppelganger domains, inbound		

	remote desktop, clear text passwords, unauthorized use of remote management tools, etc.		
28	The solution should out of the box detect use of remote management tools from non-admin devices without the need for manual tagging of devices.		
29	The solution should support analysis of network traffic without the need to decrypt and without the need for any endpoint agents or additional solutions..		
30	The solution should support tagging and annotation of 1 or more critical devices with a single operation. The solution should also support the use of these tags for the purpose of building custom threat detection or compliance models.		
31	The solution should identify ransomware, executables, and other file types that are transferred via SMB file shares. The solution should be able to create a custom file share detection model based on end user file names (SMB honeypot).		
32	The solution should detect DCERPC enumeration techniques, such as: services enumeration, computer name enumeration, domain groups enumeration, password policy enumeration, and remote file process execution.		
33	The solution should support a fully transparent and extensible language for building custom threat detections based on a minimum of 1000 network attributes including but not limited to protocol information, device information, domain information, threat intelligence etc.		
34	Automated Entity Correlation: Plug and play AI-based behavioural fingerprints for tracking entities such as devices, users and applications		
35	The solution should fully expose the definitions for all out of the box vendor provided threat detection techniques (models) and allow for their easy modification or adaptation.		
36	The solution should have the capability to distinguish between similar devices based on unique fingerprints (including unmanaged & IOT). The solution should have capability to track back to the actual traffic matching the fingerprint.		
37	The solution should have capabilities to identify historical information about all the endpoints (including unmanaged and IOT, if any) where the user has logged in without the need to integrate with any other solutions. The solution should support search for user or device names.		
38	The solution should be able to classify applications and protocols across multiple protocol families including at a minimum:		
38.1	Application Family-Description		

38.2	Antivirus-Antivirus update		
38.3	Application Service-Background service		
38.4	Audio/Video-Application/Protocol used to transport audio or video content		
38.5	Authentication-Protocol used for authentication purposes		
38.6	Behavioural-Protocol classified by non-deterministic criteria based on statistical analysis of packet form and session behaviour.		
38.7	Compression-Compression layers		
38.8	Database-Protocol used for database remote queries		
38.9	Encrypted-Encryption protocol		
39	ERP-Enterprise Resource Planning application		
39.1	File Server-File transfer protocol		
39.2	File Transfer-Protocol used for user-to-user file transfers via Instant-Messaging applications.		
39.3	Forum-Web forum		
39.4	Game-Gaming protocol		
39.5	Instant Messaging-Instant messaging application		
39.6	Mail-Email exchange protocol		
39.7	Microsoft Office-Microsoft office sub-protocol		
39.8	Middleware-Platform protocol for remote procedure calls		
39.9	Network Management-Protocol used for IT management		
39.10	Network Service-Low level network protocol		
39.11	Peer to Peer-Peer to peer application		
39.12	Printer-Printer communication protocol		
39.13	Routing-Network routing protocol		
39.14	Security Service-Workstation security application		
39.15	Telephony-Telephony core network protocol		
39.16	Terminal-Remote terminal protocol		
39.17	Thin Client-Remote control protocol		
39.18	Tunnelling-Tunnelling protocol		
39.19	Wap-Mobile specific transport protocol		
39.20	Web-Generic web traffic		
39.21	Webmail-Web email application		

40	The solution to be sized such that it supports 10 Gbps of raw packet analysis for visibility and threat hunting purposes from day one and should be able to extend to 30 Gbps on the same cluster in future whenever it is required. There should not be any restriction on number of endpoints that can be monitored.		
41	Minimum 2 nos. of hardware sensors each capable of 5 Gbps throughput to be provided that can receive traffic from different locations.		
42	The sensors will receive feed from tapAggs. TapAgg will receive feed from production network with SPAN/Mirror functionality. Minimum 3 nos of tapAgg to be provided along with to complete the solution.		
43	The TapAgg device should support multiple M:N Tap(Rx) to tool(Tx) mapping simultaneously.		
44	The tapAgg device should be capable to support same port working as tap port (Rx) and tool port(Tx) simultaneously		
45	The tapAgg device should have capability of packet truncation to remove the payload and pass on only the header (defined bytes) of the packet.		
46	The tapAgg device should be max 1RU and should have 48 nos of 1/10/25G SFP28 and 8 nos of 100G QSFP28 ports. All ports should be activated from day-1. Device should be provided with 8x 1G-T, 4x 10G-T, 16x 10/25G dual-rate SR, 8x 10/25G dual-rate LR, 4x 40G-SR4, 4x 100G-SR4 transceivers.		
47	The TapAgg device should support mixed speed port-channel i.e. active-active forwarding on LAG links consisting of multiple speeds e.g. 1G and 10G.		
48	The TapAgg device should support symmetric load-balancing, i.e. packets part of same flow but entering on different ports be load-balanced to same output port of a port-channel.		
49	The TapAgg device should have support for packet timestamping. Should support Precision Time Protocol 1588 transparent mode and boundary mode		
50	The tapAgg device should have deep packet buffers of 2GB or more to absorb burst traffic minimizing packet drops for N:1 tap port to monitor port scenarios		
51	The tapAgg device should support minimum 20K Access Control Entries for packet filtering.		
52	The tapAgg device should support policy based traffic steering towards output ports, using ACL rules.		

53	The tapAgg Device should support traffic steering based on matching inner headers fields for GRE encapsulated traffic		
54	The tapAgg device should support traffic steering based on MPLS label value.		
55	The tapAgg device should support header striping for 802.1q, MPLS, VXLAN, 802.1BR, VN-tag and GRE		
56	The tapAgg device Should have Virtual output Queue based architecture to avoid head of line blocking issues		
57	All tapAgg devices should support automation and programming with native support for bash, python, linux rpm/packages, Docker container, open config over gRPC		
58	All tapAgg devices should support bug fix/Patching without rebooting the OS.		
59	All tapAgg devices should support TACACS+, Radius and Role based access control		
60	All tapAgg devices should support redundant hot swappable Power Supplies and redundant hot-swappable fans with reversible airflow option		
61	The complete solution including NDR and tapAgg should be from single OEM for end-to-end support.		
62	The OEM professional services should perform plan, design, implementation and validation of the solution and provide onsite knowledge transfer and handover training.		
63	All the Installation need to be done by OEM and Part# for the same need to be shown in Technical Bid		
64	All the features asked should be available from day one and from same OEM. Any open source and third party solution is not All licences should be provided with the devices for the mentioned features.		

36. IPS/IDS

Sr. No.	<ul style="list-style-type: none"> Specifications for Perimeter IPS/IDS 	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
A.	Platform Requirement		
1	NIPS solution should be a purpose built dedicated standalone appliance and not a integrated firewall module or UTM appliance.		
2	Monitoring Interface should be able to operate at layer 2.		
3	The appliance must have Real World Throughput of 3 Gbps and scalable up to 7 Gbps for future requirement on the same 1 U appliance.		
4	The solution should support on the box SSL inspection.		
5	Solution must support SSL throughput of 2 Gbps from day 1.		
6	The appliance should have below port density:- 1. Fixed 8 - 1G copper ports with fail open 2. 4 - 10G SFP+ ports with internal fail open 3. Fixed 2 - 10G SFP+ ports 4 All the ports shall be fully populated with its transceivers.		
7	The appliance should have separate dedicated interface for management console. None of the monitoring ports should be used for this purpose.		
8	The proposed appliance must support 4,000,000 Maximum Concurrent Connections.		
9	The proposed appliance must support 200,000 new Connections per Second.		
10	The appliance must have redundant power supply		
B.	Detection Technology		
1	NIPS should support different mode of deployment.		

	a)IDS		
	b) TAP mode		
	c) Inline		
	d) Simulation		
2	Solution must accurately detect intrusion attempts and discerns between the various types and risk levels including Zero-Day attacks, unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids. The NIPS solution should be able to perform deep inspection of network traffic by using a combination of advanced technologies, including full protocol analysis, threat reputation and behaviour analysis to detect and protect against Zero-day attacks, malware call-backs (C&Cs), Denial of service (DoS) and other advanced threats.		
3	IPS Solution should have built-in SSL decryption Engine for SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured http channel without need to have additional appliances.		
5	The IPS Solution should support Anti-malware protection through various engines as part of solution offerings.		
6	The IPS Solution should have real time emulation techniques for embedded malware protection.		
7	IPS appliance should provide advanced DoS detection with "self learning" for more accurate and fewer false positives.		
8	The IPS must support IPv4 and Ipv6 from day-one and detect attacks inside IPv6 encapsulated packets		
9	IPS should provide protection from evasion based attacks		
10	The solution should have Anti-spoofing capabilities		
11	should have capability for Host quarantine and rate limiting		
12	IPS must support high availability in Active-active and active-passive mode with stateful failover and not only limited to transparent mode.		

13	<p>IPS must support protocol tunnelling for following:-</p> <ul style="list-style-type: none"> ■ IPv6 ■ V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels ■ MPLS ■ GRE ■ Q-in-Q Double VLAN 		
14	<p>NIPS should support provide advanced botnet protection using following detection methods:-</p> <ul style="list-style-type: none"> ■ DNS/DGA Fast flux call back detection ■ DNS sink holing ■ Heuristic bot detection ■ Multiple attack correlation ■ Command and control database 		
15	<p>Should protect against DOS/DDOS attacks. Should have "self-learning" capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network:-</p> <ul style="list-style-type: none"> ■ Threshold and heuristic-based detection ■ Host-based connection limiting ■ Self-learning, profile-based detection 		
16	<p>Solution should be able to control traffic based on geographical locations -- For e.g. a policy can be created to block traffic coming or going to a particular country. Provision should be there to allow specific IPs for any blocked country</p>		
17	<p>Solution should have the capability to create Black List rules and White List rules which should allow to block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.</p>		
c	Advanced Prevention and Response		
1	<p>IPS Solution must have capability to PRIORITIZE risk of threats to you with Campaigns detected and IP addresses that could be exposed</p>		

2	IPS should have capability to act as an additional source of threat information for Prioritization and predictive threat hunting solution in a way that it can share the telemetry data for predictive analysis.		
3	IPS must have capability to quarantine user endpoint machine if it is communicating with bad vectors		
4	IPS must have capability to provide detailed host machine context at central dashboard		
5	IPS must support Inbound SSL Inspection detection and prevention using dynamic agent based key for ECDHE cypher suits		
7	IPS must have multiple signature less engines on the appliance without degrading the performance.		
8	Solution must have dedicated emulation engine to provide protection from advanced attacks.		
9	IPS must support on demand throughput scalability by just upgrading software license-Scalable on demand throughput based scalability without changing the hardware		
10	IPS must support Advanced Analytics, Heuristics and Machine Learning		
11	IPS must provide communication fabric based integration with multiple other existing solution such as immediately share relevant data between endpoint, gateway, and other security products enabling security intelligence and adaptive security.		
12	IPS must have inbuilt network behavioural analysis engine to provide additional context using network flows.		
13	NIPS should support High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained.		
14	NIPS should support Active-Active high availability. The HA should be out of the box solution and should not require any third party or additional software for the same		
15	NIPS should be able to perform entire packet capture of the traffic and sent to the manager for analysis		

D.	Management		
1	Solution should manage the NIPS appliances from a central management console		
2	Management platform supports policy configuration, command, control, and event management functions for the NIPS appliances		
3	Management console should support Radius and LDAP authentication in addition to the local user authentication		
4	Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks		
5	NIPS Management console should support high availability which should have Automated failover and fail-back		
6	<p>NIPS solution should provide Intelligent security management:-</p> <ul style="list-style-type: none"> ■ Intelligent alert correlation and prioritization ■ Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ Scalable web-based management 		
7	NIPS Management console should be capable of producing extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		
8	It must have memory dashboard details memory utilization by device		
E.	OEM Support		
1	Bidders must address Problems in equipment which cause downtime/degradation of services and resolution of which require development of patches, bug fixes etc. shall be treated, by Security products OEM, on priority basis.		
2	Bidder must provide Schedules and performs Quarterly on-site visits; completes Protection Analysis and offers best practices recommendations.		

3	Bidder must provide Proactive notification of malware threat advisories and product updates		
F.	Feature Support		
	All the features asked should be available from day one and from same OEM. Any open source and third party solution is not accepted		

37. SSL VPN Gateway

S.No.	Minimum Requirement for SSL VPN Gateway	Marked/ Cross Reference Specification with reference page no.	Highlighted Reference of with	Compliance (Yes/No)
1	The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW/ ADC device It should have should have 1x1GbE port for management and 8x10GbE SFP+ ports with its transceivers.			
2	The appliance should have multicore CPU, 64GB RAM, 4TB HDD and dual power supply.			
3	The solution Should have dedicated hardware SSL card and should support 45 Gbps of SSL Throughput			
4	The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 10000 concurrent users on the same appliance without changing any hardware			
5	The device should support on demand provisioning of L3 VPN client using ActiveX or JAVA applet, standalone and command line L3 VPN client support.			
6	The solution should support different network pools defined per user or group.			

7	The appliance should support 45 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software. Proposed appliance should support Desktop over VPN feature to provide access to desktop from remote for WFH purpose.		
8	The solution should support desktop publishing on IOS and Android phones along with device ID based authorization. The solution should support enterprise App-store for android and IOS phones. The solution should support SDK for IOT devices. Should also support SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine authentication based on combination of HDD ID, CPU info and OS related parameters, mac address to provide secure access to corporate resources.		
9	The solution should support following Authentication methods:		
10	a) Active Directory, b) LDAP , c) RADIUS ,d) Local database e) SAML f) Google O-Auth Support g) SMS		
11	The solution must provide ranking of at least 4 authentication methods for granular authentication of VPN users		
12	Appliance must support Access control options based on:-		
13	a) User and group, b) Source IP and network, c) Destination network ,e) Service/Port, f) Host name or IP address ,g) IP range, h) Subnet and domain, I) Day, date, time and range		
14	Should have IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support. Also should have IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation based health check for intelligent traffic routing and failover. Solution should support full DNS server functionality to support all kind of DNS records including A,AAAA, MX, CNAME, PTR DNS records.		

15	The solution should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode using standard VRRP (RFC-2338) for HA interconnection over network. Should support both device level and VA level High availability.		
	All the features asked should be available from day one and from same OEM. Any open source and third party solution is not accepted		

38. Active Directory Solution

Description	Specification	Marked/ Cross Reference Specification reference page no.	Highlighted Reference of with	Compliance (Yes/No)
Device's support required	2500 or higher			
User support	1000			
Hardware & Software	SI must provide desired hardware and software to meet solution requirement			
User Management	User life cycle management.			
	Create, modify, move, unlock, enable/disable, delete, and restore the Single/Bulk Users without using any manual scripts.			
	User Self Service portal to reset password and to unlock the account on their own.			
	Delete the accounts automatically on expiry of validity period			

	Automatically lockdown privileged accounts that are inactive for a period of time.		
	Create privileged roles for task delegation and Audit the actions performed by these Delegates, including what action was performed on what object and when.		
	Allow users to request access to privileged groups.		
	Enhance security of privileged accounts by enabling multi-factor authentication.		
	Protect privileged accounts from password attacks by enabling advanced password policy requirements, including a dictionary rule		
Computer Management	Create, modify, move, manage, enable/disable, delete, and restore the Single/Bulk Computers without using any manual scripts		
DNS Functionality	Yes		
Group Management	Create, modify, move and delete the Single/Bulk Groups without using any manual scripts.		
Group Policy Objects(GPO) Management	Create, modify, and manage the GPOs. Link the GPOs to users/Computers/Groups/OUs		
Delegation Management	Define the roles for User, Technician and Admin. Provide restricted privileges for a Technician to perform only specific tasks/roles.		

Administrator Management	Review-Approve facility for all admin activities. Privileged access for Users		
Clean up	The cleanup should be configured to run every month are as and when required to remove the users based on certain conditions and consolidated task reports to be sent to relevant stakeholders upon cleanup.		
Role-based access and privileged	Should be configurable with roles that can be used to delegate task to help desk technician and other department members		
Integration with other related systems	Yes, to achieve the required functionality such as for RBAC,DNS, etc.		
Backup and recovery	Facilitate backup of entire Active Directory setup including users and rights data		
	Automates the entire recovery process, including rebuilding the global catalogue & FSMO Role DCs		
	Support Active directory bare metal recovery. Recovery solution must be enabled with automated backups, quick compare of backup to current values of AD to pinpoint differences, and instantly recover the desired data Solution should be able to restore entire forest from single console		
High Availability	Yes		

39. Console Management Server

S.No.	Specification	Marked/ Cross Reference of Specification with reference page no.	Highlighted Compliance (Yes/No)
	Remote OOB Network Management Solution		
1	SI is responsible for overall SITC of all components of the solution which include hardware, software and accessories required for the solution to meet desired outcomes.		
2	The Solution shall be industrial-grade and comply with the following requirements: 1) Dual-core ARM Cortex-A9 MP Core with Core Sight 2) 1GB DDR3L RAM 3) 16GB eMMC Flash 4) 2 Gigabit Fiber SFP ports 5) 10/100/1000BT) Ethernet interfaces on RJ45		
3	The equipment must support dual AC power supply for ALL Rack Mounted Devices.		
4	Solution should provide secured Serial access to remote network devices over IP along with Fast, automated configuration with Zero Touch Provisioning		
5	The OOB equipment must support Serial (48 ports), Ethernet and SFP connections.		
6	The Solution should provide combination of USB and RJ45 serial ports for target network devices		

7	The solution should support vendor agnostics and to be compatible with Serial and Ethernet connections of target devices from various network vendors.		
9	Both hardware and software components of the solution will have built-in Firewall for additional security which can restrict services to any interfaces, brute-force protection.		
10	<p>Console Management -</p> <ul style="list-style-type: none"> .Sun break-safe (Solaris Ready Certified) .Break-over SSH support .Off-line data buffering – local and remote (NFS/Syslog/OEM management software) .Level-based syslog filters .Time stamp and rotations for data buffering Unlimited number of simultaneous sessions Simultaneous access on the same port (port sniffing) with ability to toggle .Configurable event notification (e-mail, pager, SNMP trap) .Customizable, global time zone support . Multiple and customizable user levels of access 		

11	<p>Security –</p> <ul style="list-style-type: none"> .Preset security profiles–secure, moderate and open Custom security profiles .X.509 SSH certificate support .SSHv1 and SSHv2 .Local, RADIUS, TACACS+, LDAP/AD, NIS and Kerberos authentication . Two-factor authentication (RSA SecurID®) .One-Time Password (OTP) authentication .Local, backup-user authentication support PAP/CHAP and Extensible Authentication Protocol (EAP) authentication (for dial-up lines) <p>Group authorization:</p> <ul style="list-style-type: none"> TACACS+, RADIUS and LDAP • Port access • Power access • Appliance privilege <ul style="list-style-type: none"> • IP packet and security filtering User-access lists per port System event syslog IPsec with NAT traversal support IP forwarding support Secure factory defaults Strong password enforcement 		
12	<p>Port Access –</p> <ul style="list-style-type: none"> Directly by server name or device name CLI Command Simultaneous Telnet and SSH access HTTP/HTTPS 		

13	System Management – Configuration wizard in Web for first-time users Auto-discovery for automatic deployment Command line interface (CLI) Web Management Interface (HTTP/ HTTPS) SNMP Internal temperature sensor Upgrades available on FTP site, no charge TFTP support for network boot		
14	The Solution must be able to provide remote power reset capability (reboot) of targeted devices when integrated with IPDU.		
16	The solution must be capable of integrate with PDU major vendors		
17	The management platform/Software to be provided along with hardware which should support windows and Linux installation		
18	The management platform shall provide a single pane of glass, to access to any devices that is connected to it by means of secure CLI or IP access		
19	OEM or Manufacturer should be ISO 9001: 2000, ISO 14001 , ISO/IEC 27001:2013 and ISO 45001 certified.		
20	Emissions, Immunity and Safety:		
	• FCC Class A		
	• UL		
	• CE Class A		
	• EN-60950		
Feature Support	All the features asked should be available from day one		

40. KVM Console

Sr.no	Technical Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Proposed 18.5" LCD console tray and 16 port IP KVM switch should be built in design and should occupy 1U space together in 19" standard rack.		
2	It should have cable management arm(CMA) and the 16x RJ45 port KVM switch built in at the rear side of the LCD console tray to save the U space in Rack.		
3	Both LCD console tray and the built-in KVM switch should have separate power supply.		
4	Vendor should supply 16 number of KVM cables with VGA, USB connectors.		
5	KVM cables should have LEDs to indicate Power and connection status.		
6	Built-in KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt		
7	Supplied KVM cables should support Virtual media to map USB media devices to target servers remotely over TCP/IP and Smart Card(CAC).		
8	Built it KVM switch should have encryption 128-bit AES for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication.		
9	KVM Session should support Keyboard pass through.		
10	Built-in KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable.		
11	Built-in KVM switch should not have power on/off switch to avoid accidental and unnoticed power off.		
12	Built-in KVM switch should have two local console ports. One to connect with the LCD console tray and another for external Monitor and keyboard connection for any emergency local access.		
13	LCD display should support brightness 250 cd /m2, contract ratio 1000:1 and 16.7million colors.		
14	LCD console tray and built in KVM switch should support max resolution 1600 x 1200 at 60 Hz.		
15	Operating temperature and Humidity of LCD console tray should be 0°C to 50°C and 10% to 80%		
16	LCD console tray should have 103 key keypad with number pad and touchpad.		

17	It should have control buttons on the front of the monitor to adjust the characteristics of the image that is displayed.		
18	It should have two independent USB 2.0 compliant pass through ports at front side.		
19	LCD console tray should be global certified by most of the agencies like UL, CE, CCC, BSMI, C-Tick, EAC, VCCI, KCC , FCC Class A		
20	Bidder should provide two (02) ethernet cable with each KVM. It should be noted that of each ethernet cable should be atleast equal to the cater the distance two adjacent racks in left and two at its right side		
21	All the features asked should be available from day one		

41. Portable KVM console adapter

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Laptop USB Console (LUC) Port	1 x RJ45 Male		
KVM (Computer) Ports	1 x USB Type A Male		
	1 x VGA Male (Blue)		
LEDs	1 (Blue)		
USB bus-powered design and supports 1920 x 1200 @ 60 Hz video resolution	yes		
Instant BIOS-level access and no software installation	yes		

42. Monitoring and management tool for servers

S.No.	Specifications:	Marked/ Highlighted Reference Specification with reference page no.	Cross of with Compliance (Yes/No)
1	The solution should be deployed at DC and DR working in HA and supplied with all the associated hardware		
2	Access device-level lifecycle management with a single click—no need to navigate among appliances with license to add up to 4000 servers		
3	User defined policy/ template based automated and simultaneous operations like: <ul style="list-style-type: none"> - OS deployment - Firmware update - BIOS update - Server cloning - Creation of Virtual disks along with RAID configuration - Network configuration - Web server and SSH and configuration - Secure erase of storage drives 		
4	Redfish, Restful API support for automated management		

5	<p>Monitoring of multiple aspects of servers like:</p> <ul style="list-style-type: none"> - Server power consumption - Health - Storage (Physical & Virtual) - Cooling - CPU - Intrusion - Network device(s) - Multiple components voltage readings (e.g. CPU, system board, PSU, etc.) 		
6	<p>Integrated reporting to see server hardware & firmware inventory (of all hardware and software components), including associated firmware versions along with option to create customized reports</p>		
7	<p>Fault management: Get monitoring, pre-failure alerts, failure alerts, log (system events, lifecycle, troubleshooting, user session, etc.) monitoring & extraction, automatic call logging (configurable), status monitoring of trouble ticket and contract/warranty registration & display for each device</p>		
8	<p>Should have management features like:</p> <ul style="list-style-type: none"> - Power management and configuration - Virtual Console with management features like boot selection, power on/off, virtual media, virtual clipboard, etc. - Asset Tracking - Server profile import/export - Role based user management with feature for integration with LDAP(AD),AAA - Time-zone/NTP 		
9	<p>Blink LED to identify a particular server</p>		
10	<p>Software and Hardware for this Monitoring and management tool for servers shall be provided by the OEM of servers.</p>		
11	<p>All the features asked should be available from day one</p>		

43. Fireproof Vault

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Volume (Litres)	200 or more		
Type	Fire Resistant Safe, inner temperature remain at less than 118°C even while exposed to a flame of 1,030°C for an hour		
Lock type	Electronic		
Security	Dual Combination Mode(User Password & Mechanical Key)		
High Security Emergency Key	Yes(Unlock possible with mechanical keys when PIN lost)		
Auto Secure Mode	Yes (mechanical keys &Password)		
Certifications	UL Fire Rated, Conforms to UL Test Standards		

44. Degausser

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Media Handling:	Standard PC, Laptop and Server 3.5", 2.5" & 1.8" Hard Drives.		
Longitudinal & perpendicular recording	Up to 2TB.		
All drive interfaces	IDE, SATA, SAS and Fibre Channel.		

Power Supply	220-240V 50Hz		
Degaussing Force	7000 Gauss		
Duty Cycle	20%		
Erasure Depth	-75dB on 1500 OE Tape, -90dB on 750 OE Tape		
Throughput	20 Hard drives or 40 tapes per hour typical		
Controls	On/Off, Security Key		
Indicators	On/Off Erase Field, Coil Power Supply Warning Light		

45. Data Diode

Specification	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Salient Features	Unique hardware bases one way communication at physical layer. MAC address-based selection of source at Data Diode Promiscuous mode Easy to use GUI for configuration and log management 19 inch Rack mountable		
Allowed MAC address	100 no. of source MAC		

Network Ports	01no. INGRESS and 01no. EGRESS Ethernet port. 1G optical Ports for INGRESS and EGRESS populated with SFPs (optical/electrical), 01no. MGMT/LOG Ethernet port		
Management/ Status	Ethernet based IP address configuration		
Input voltage	230VAC @ 50Hz , operating environment -10 deg C to 60 deg C		
EMI/EMC	FCC part 15 Class A		
Physical Security	Tamper Evident		
Logging	Syslog based		
Protocols Support	Protocol agnostic (any unidirectional), Syslog, Netflow		
Feature Support	All the features asked should be available from day one		

46. & 49. Intelligent Cabling

Cabling Structure is as follows at DC & DR:

Network-1,100G Network:

- There are Two Spine Switch-Primary and secondary.
- Each spine switch will have 120 X 100G port (Total 2 X 120, 100G port).
- 48 MPO port to be established between Primary and secondary spine rack for connecting Network/routing devices.
- 48 each MPO port to be established within (Primary and secondary) spine rack for connecting Network /routing devices.
- At Server/storage rack end, there will be one no.s of 48 port Leaf switches.
- Each Leaf switch will have 1 X 100G MPO connectivity from Spine switch (Primary & Secondary) Total 2 X 100G connections.
- Each Leaf switch will have 48X 10G on fiber, out of which maximum 32 ports will connect to server/storage (i.e 16 ports will connect to same rack's server ports and remaining 16 ports will connect to adjacent rack server's ports).
- The rows with odd no. of Racks, in such case Last Rack will have dual leaf switch and each leaf switch will have 2x100G MPO connectivity from Spine switch (Primary & Secondary) Total 4 X 100G connections.
- 2 LC Duplex connections will be extended to each Server/Storage via fiber shelf to enable intelligent solution.

Network-2,10GNetwork:

- There are Two Core Switch-Primary and secondary
- Each Cores switch will have48 X10G port
- 24 LC port to be established within Primary and secondary core rack for connecting Routing/Network.
- At Server/storage rack end, there will be one 48 copper port edge switch to support 10G from core switch.
- Edge switch will have 1X 10G LC connectivity from core switch (Primary & Secondary) Total 2X 10G connections
- Edge switch will have 48 X 1G on copper to connect server/storage, out of which maximum 24 ports will required to connect server/storage of the rack.
- 24 Copper connections will be extended to Server/Storage via copper panel to enable intelligent solution.

-

- The Top of Rack (ToR) switch in the S/R will connect to the Spine switch (in N/R) via 12F (1 x 12 MPO connectors on each side) MPO trunk cables on OM5. All MPO trunk cables and MPO cable assemblies shall be Method B polarity only. The adapters shall be compliant to TIA/EIA FOCIS 5, which is commonly referred to as “aligned keys” or “key-up to key-up.” Each link between the ToR and Spine shall support 100GBASE-SR4 application for the complete channel. Contractor shall check and guarantee the support of 100GBASE-SR4 application for the longest distance possible between the existing network rack and new server rack (part of the additional 70 S/R) inside the data center. All patch cords required to complete the connectivity shall be standard compliant. In the event due to unavailability of the patch cords, patch cords from other OEMs with similar specifications shall also work in the system.
- Each edge switch will connect to the core switch (N/W) via 12F (1 x 12 MPO connector on each side) MPO trunk cables on OM4. Each link between the edge and core Switch shall support 10GBASE-S application for the complete channel. Contractor shall check and guarantee the support of 10GBASE-S application for the longest distance possible between the existing network rack and new server rack (part of the additional 70 S/R) inside the data centre. All patch cords required to complete the connectivity shall be standard compliant. In the event due to unavailability of the patch cords, patch cords from other OEMs with similar specifications shall also work in the system.

Product specification for 100G MPO Connectivity- OM5 components

Deploy optical fiber pre-terminated solution consisting of trunk cables with pre-terminated MPO connector, cassettes, patch cords and optical fiber patch panels etc. as a standard configuration. The entire component shall be intelligent enabled solution. The fiber count per MPO trunk cable shall be 12F MPO pinned connectors on either sides) The application shall support up to 10/40/100/400G. The fiber shall be multimode OM5 fiber features extended bandwidth range of 850 to 950nm that enables it to provide optimal support to SWDM applications by enhancing its capability to transmit at least four low-cost wavelengths for longer distance, reducing parallel fiber count by four-folds and high-speed application of 400G. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

a) Fiber Patch cord assembly OM5 MPO to MPO, Male/Female

S. N.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
3	Fiber Type			
4	Interface Feature,			
5	Total fiber quantity			
6	Jacket color	Lime green		
7	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
8	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Single sheath jacket		
9	Flame Test Method	IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE-383,		
10	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409,		
11	Safety Standard	UL 1666, UL 1685 / BIS or equivalent Standards		
12	Insertion Loss Change, mating	0.3 dB		
13	Return Loss, minimum	27dB		
14	Insertion Loss Change, temperature	0.3 dB		
15	Insertion Loss, maximum	0.25 dB		
16	Intelligent compatibility	Patch cord shall be compatible for intelligent solution		
17	RoHS	RoHS Compliant		

b) Fiber Distribution adaptor OM5, MPO Port

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
	Interface Feature, rear			
4	Port Duct cover	No		
5	Standard	MPO distribution adaptor shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
6	Safety Standard	UL/ BIS or equivalent Standards		
7	Intelligent compatibility	Distribution adaptor shall be modular type and Intelligent enabled		
8	Fiber Type	OM5.		
9	Qualification Standards	IEC 61753-1 TIA-568.3-D		
10	RoHS	RoHS Compliant		

c) Fiber Trunk cable assembly OM5 MPO (Male/Female) to MPO (Male/Female)

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
3	Interface Feature,			
4	Total fiber quantity			
5	Panel compatibility			
6	Cable compatibility			
7	Fiber Type	OM5		
8	Jacket color	Lime green		

9	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
10	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Double sheath jacket for more protection		
11	Cable strength member	Ripcord and Aramid Yarn shall be included as cable protection		
12	Flame Test Method	IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE-383,		
13	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409,		
14	Safety Standard	UL 1666, UL 1685/ BIS or equivalent Standards		
15	Insertion Loss Change, mating	0.3 dB		
16	Return Loss, minimum	27dB		
17	Insertion Loss Change, temperature	0.3 dB		
18	Insertion Loss, maximum	0.25 dB		
19	RoHS	RoHS Compliant		

d) LC type fiber patch cords, OM5

S. N.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Fiber type	Multimode OM5		
2	Construction	Two fiber duplex Cordage Non-armored gel free cable		
3	Cable Sheath	Low Smoke Zero Halogen (LSZH) Riser rated		
4	Connector type	LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser		
5	Cable Length	As per the BOQ		
6	Color	Lime Green color for cable and Gray color for connector		
7	Protection	Aramid yan shall be provided around 250nm fiber cable		

8	Minimum Bend Radius	38 mm (Loaded), 15mm (Unloaded)		
9	Tensile Load, maximum	20N (long term) 67N short term)		
10	Compression	10 N/mm as per IEC 60794-1 E3 test method		
11	Ferrule	Pre-radiused made of Zirconia		
12	Cable Qualification Standards	ANSI/ICEA S-83-596, Telcordia GR-409		
13	Flame Test Listing	NEC OFNR-LS (ETL) and c(ETL)		
14	Flame Test Method	IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666, UL 1685/ BIS or equivalent Standards		

e) Intelligent fiber panel- MPO type, OM5

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Intelligent fiber Patch panel shall be modular, accept cassette type module and distribution adaptor pack for multimode (OM5) type fiber		
2	Standards	Intelligent panel should meet ANSI/TIA 568C.2 specifications and AIM standard such as ISO/IEC 18598 and TIA 606-B and ISO/IEC 14763-2.		
3	LC Port capacity	Intelligent pre-terminated fiber shelves shall be available in 1U sliding configuration to support up to 48 -duplex LC ports or 2U sliding configuration to support up to 144 -duplex LC ports		
4	MPO Patch connections	Intelligent fiber patch panels shall be available in 1Usliding configurations with up to 32 MPO ports, in 2U sliding configuration to support up to 96 MPO ports. Requirement of 1U/2U in each rack shall be assessed by bidder.		
5	Patch cord compatibility	Intelligent patch panel shall provide a button and an LED indicator at every panel port to enable easy tracing and identification of patch connections in the telecom room.		
6	Sensing Assembly Installation	Intelligent patch panels shall be provided with all necessary system-connecting cable(s).		

7	Connection of existing port	Intelligent fiber patch panels should allow for removal and replacement of sensing Assembly. Any fault in the sensor should not disrupt the operation of panel network port.		
8	Patch cord/wire manager	Panel shall have inbuilt rear cable manager and from patch cord manager including visible label plate		
8	RoHS	RoHS Compliant		

f) Any other item required to complete the OM5 Intelligent cabling - To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. N.	Details	Standard Compliance	Compliance (Yes/No)
1	Any other item required to complete the OM5 Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

Product specification for 10G MPO Connectivity- OM4 components

Deploy optical fiber pre-terminated solution consisting of trunk cables with pre-terminated MPO connector, Fiber modular cassette with LC interface, 2F LC -LC patch cords and Intelligent fiber patch panels as a standard configuration. The entire component shall be intelligent enabled solution. The application shall support up to 10/40G. The fiber shall be multimode OM4 fiber. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

g) Fiber trunk cable assembly OM4 MPO (male/Female) to MPO (male/Female)

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
3	Interface Feature,			
4	Total fiber quantity			
5	Panel compatibility			

6	Cable compatibility			
7	Fiber Type	OM4		
8	Jacket color	Aqua Color		
9	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
10	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Double sheath jacket for more protection		
11	Cable strength member	Ripcord and Aramid Yarn shall be included as cable protection		
12	Flame Test Method	IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE-383,		
13	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409,		
14	Safety Standard	UL 1666, UL 1685// BIS or equivalent Standards		
15	Insertion Loss Change, mating	0.3 dB		
16	Return Loss, minimum	27dB		
17	Insertion Loss Change, temperature	0.3 dB		
18	Insertion Loss, maximum	0.25 dB		
19	RoHS	RoHS Compliant		

h) Fiber Distribution fiber panel, Modular, OM4 LC

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
3	Interface Feature, rear			
	Panel compatibility			

	Cable compatibility			
4	Port Duct cover	Yes		
5	Standard	Fibre distribution fiber panel shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
6	Safety Standard	UL/ BIS or equivalent Standards		
7	Fiber Type	OM4 Multimode		
8	Intelligent compatibility	Fibre distribution fiber panel shall be modular type and Intelligent enabled		
9	RoHS	RoHS Compliant		

i) Fiber Modular Cassette OM4 MPO – LC

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	To be asses by Bidder		
2	Interface and port			
3	Interface Feature, rear			
4	Panel compatibility			
5	Cable compatibility			
6				
7	Port Duct cover	Yes, must required		
8	Standard	MPO cassettes shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
9	Safety Standard	UL/ BIS or equivalent Standards		
11	Approximate dimension	25mm (H) X 95mm (W) X 115mm (D)		
12	Fiber Type	OM4 Multimode		

13	Attenuation	1.00 dB/km @ 1,300 nm 2.20 dB/km @ 953 nm 3.00 dB/km @ 850 nm		
14	Insertion Loss Change, temperature	0.3 dB		
15	Insertion Loss, maximum	0.47 dB		
16	Intelligent compatibility	Fiber Cassette shall be modular type and Intelligent enabled		
17	RoHS	RoHS Compliant		

j) LC type fiber patch cords, OM4

Sl. No.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Fiber type	Multimode OM4		
2	Construction	Two fiber duplex Cordage Non-armored gel free cable		
3	Cable Sheath	Low Smoke Zero Halogen (LSZH) Riser rated		
4	Connector type	LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser		
5	Cable Length	As per the BOQ		
6	Color	Aqua color for cable and Beige color for connector		
7	Protection	Aramid yan shall be provided around 250nm fiber cable		
8	Minimum Bend Radius	38 mm (Loaded), 15mm (Unloaded)		
9	Tensile Load, maximum	20N (long term) 67N short term)		
10	Compression	10 N/mm as per IEC 60794-1 E3 test method		
11	Ferrule	Pre-radiused made of Zirconia		
12	Cable Qualification Standards	ANSI/ICEA S-83-596, Telcordia GR-409		
13	Flame Test Listing	NEC OFNR-LS (ETL) and c(ETL)		
14	Flame Test Method	IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL1666, UL 1685/ BIS or equivalent Standards		

15	Insertion Loss, maximum	0.3 dB		
16	Return Loss, minimum	27 dB		
17	Regulatory Compliance	RoHS 2011/65/EU compliant		

k) Any other item required to complete the OM4 Intelligent cabling – To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. N.	Details	Standard Compliance	Compliance (Yes/No)
1	Any other item required to complete the OM4 Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

Product specification for 1G/10G Copper components

Deploy Copper cabling solution consisting of single ended copper patch cord with RJ45 male connector, intelligent Copper patch panel, reduced diameter patch cords for high density connecting servers as a standard configuration. The entire component shall be intelligent enabled solution. The application shall support up to 1/10G. The copper solution shall be Cat-6A U/UTP cabling. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

I) CAT 6A Intelligent Patch Panel

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Patch panel Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A		
2	Standards	The panel should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Panel configuration	The panel shall be available in 24-port and 48-port configurations with universal A/B labeling and 110 connector terminations on rear of panel allowing for quick and easy installation of 22 to 24 AWG cable		
4	Material used	Panel shall be available in straight with made of Powder- coated steel. Color shall be Stain chrome		
5	Intelligent system	The panel must be an intelligent system		
6	Additional future for noise cancellation	Termination managers must be provided with the panel. These termination managers provide proper pair positioning, control, and strain relief features to the rear termination area of the panel.		
7	Third party certificate for Genunity	ETL four connector channel certificate for long distance and short distance test report.		
8	Rear cable manager	Panel shall have rear cable manger with proper design to hold all 24 cable. This shall provide strain relief for outlet and organization of cables being routed to the back of a patch panel.		

9	RoHS	RoHS Compliant		
10	Patch Panel Ports	To be assessed by bidder to connect 48 port OoB Switch and other respective units (server and Leaf Switch)		

m) CAT 6A LSZH U/UTP RJ45 regular Patch Cords

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A patch cords		
2	Standards	The Cordage should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Length	The cordage shall be available in different length based on the site requirement		
4	Conductor	Copper must be solid single strand copper conductor for panel termination		
5	Fire Safety standards:	LSZH		
6	Diameter Over Jacket	7.24 mm		
7	Safety Standard	UL 1863/ BIS or equivalent Standards		
8	Additional info	The cable and cordage shall be UTP components that do not include internal or external shields, screened components or drain wires that require additional grounding and bonding		
9	RoHS	RoHS Compliant		

n) CAT 6A LSZH U/UTP RJ45 reduced dia. Patch Cords

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A patch cords.		
2	Standards	The Cordage should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Length	The cordage shall be available in different length based on the site requirement		
4	Fire Safety standards:	LSZH		
5	Diameter Over Jacket	4.95 mm 0.195 in		
6	Safety Standard	UL 1863/ BIS or equivalent Standards		
7	Additional info	The cable and cordage shall be UTP components that do not include internal or external shields, screened components or drain wires that require additional grounding and bonding		
8	RoHS	RoHS Compliant		

o) Any other item required to complete the Copper cabling - To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. N.	Details	Standard Compliance	Compliance (Yes/No)
1	Any other item required to complete the Coper Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

47. & 50 Intelligent (AIM) system Monitor

SI No	AIM System Monitor at Rack level	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The AIM System Monitor shall be compatible with mounting on 19" (width) based hardware per EIA-310.		
2	The AIM System Monitor shall provide capability for a technician to communicate with AIM System Software component.		
3	The AIM System Monitor shall communicate with the AIM-enabled patch panels in the racks		
4	The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor per server rack or one monitor for two Server racks, as per system capability.		
5	The AIM System Monitor shall be able to display on the screen information indicating if a traced panel port is assigned to a scheduled work order.		
6	The AIM System Monitor shall be able to display electronic work orders for moves, adds and changes (MACs).		
7	The AIM System Monitor shall have a configurable Ethernet LAN connection capability (10BASE-T, 100BASE-TX or 1000BASE-T) to enable communication with AIM System Software component.		
8	AIM System Monitor should be fully Integratable with existing AIM system software at DC for seamless operation.		
9	Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.		
10	All the features mentioned above should be available from day one		

48. & 51 Intelligent (AIM) system Software

SI No	Intelligent System (AIM) Software defined by the ISO/IEC 18598 standard	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The AIM System Software component shall be web based.		
2	The system should support: <ul style="list-style-type: none"> a. 12000 ports or higher at DR. b. For DC, 10000 Ports from existing AIM System software OEM and upgrade the hardware as required. c. Or 15,000 Ports from New OEM Provider. New OEM provider must integrate its AIM solution with existing AIM solution. d. AIM solution software and its hardware should be from same OEM. 		
3	The AIM System Software component shall be compatible with Simple Network Management Protocol (SNMP) and support SNMP v1, SNMP v2c, and SNMP v3.		
4	The AIM System Software component shall support IPv4 and IPv6 communications.		
5	The AIM System Software component shall support automatic and manual database backups.		
6	The AIM System Software component shall have capability to auto discover the installed AIM hardware component (intelligent panels and control systems) in each rack/cabinet and to auto populate this information in its database.		
7	The AIM System Software component shall have the capability to auto discover networked devices that are connected to the pre-defined managed network switches (LAN and SAN environments) and then to auto populate that information in its database.		
8	The AIM System Software component shall provide end user with ability to define manual, automatic, or disabled mode for conducting discovery of networked devices. The automatic device discovery feature shall allow end user to determine a polling schedule, as well as the ability to automatically trigger the discovery process based on SNMP link-up traps from managed network switches.		

9	The AIM System Software component shall have the capability to auto discover IP address, MAC ID, WWN and Host Name information for networked devices and then to auto populate this information into its database.		
10	The AIM System Software component shall have the capability to auto discover networked devices with multiple MAC addresses (i.e., servers with multiple NICs, virtual machines, wireless APs, IP phone/computer pairs, etc.) and then to auto populate that information in its database.		
11	The AIM System Software component shall have the capability to auto discover VLAN ID information on managed network switches and then to auto populate that information in its database.		
12	The AIM System Software component shall provide the ability to define type of networked devices based on MAC or IP address range that could also be applied retroactively to already discovered devices. Once defined, each device upon its discovery shall be automatically labeled and represented with an appropriate icon in the database to correspond to the device type definition.		
13	The AIM System Software component shall have the capability to detect configuration changes to managed SAN and LAN switches.		
14	The AIM System Software component shall have the capability to detect when a networked device has moved or changed its physical location.		
15	The AIM System Software component shall provide capabilities for defining a set of specific system conditions that need to be tracked.		
16	The AIM System Software component shall provide a dedicated service-provisioning feature for servers, including server templates, and graphics to allow for efficient planning and deployment of servers in the data center.		
17	The AIM System Software component shall provide a server decommissioning feature that ensures removal of all circuits connected to the server to eliminate "dormant" connections.		
18	The AIM System Software component shall have the capability to document various topologies (zone, pod, cell, etc.) for Data Center applications.		
19	The AIM System Software component shall have the capability to audit the switch ports.		
20	The AIM System Software component shall have the capability to send an email message to specified personnel, to automatically execute a designated program		

	or to send a SNMP trap to a destination server each time a pre-defined system event is received.		
21	Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.		
22	All the features mentioned above should be available from day one		

52. Smart Rack

S. No	Description of Requirements	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Scope of Work		
1.1	Intelligent Integrated Infrastructure with inbuilt hot and cold aisle containment of 1 rack should cater IT load up to 6 KVA with minimum 24 U usable space available for IT equipment(s).		
2	Requirements		
2.1	Intelligent Integrated Infrastructure with inbuilt hot and cold aisle containment of 1 rack catering IT load up to 6 KVA .The Critical systems like rack-mounted air-conditioning & UPS systems should have N+N topology respectively.		
2.2	The critical components like Cooling unit , UPS,Rack, electronic door access, auto door opening system & Monitoring unit should be from same & single OEM for better integration & service support .		
3	The Intelligent integrated Infrastructure shall have following components:-		
3.1	Rack based closed loop Air-Conditioning (6 kW - 01 no. with N+N redundancy)		
3.1.1	Rack based Air Cooling with indoor - out door design, SHR >0.9, 100% Duty cycle, auto controlled Compressor, zero U rack mountable, Electronically commutated centrifugal evaporator fan , High Pressure & Low Pressure protection , Washable filter with 80% efficiency down to 20 micron , Hydrophilic evaporator coil, ON/OFF switch at indoor unit for emergency purpose, R407C/R410A Refrigerant.		

3.1.2	<ul style="list-style-type: none"> The Cooling Unit should not consume any U space. Cooling unit should have two cooling circuits and controllers inside the internal unit & external to ensure automatic changeover in the event of a failure. It should be able to support indoor to outdoor piping as below: <ul style="list-style-type: none"> a.Up to 15 mtr. horizontally b.25 mtr (5 mtr vertical + 20 Mtr horizontal) 		
3.2	UPS System - 02 Nos in N+N redundancy		
3.2.1	UPS should be of True On-line, Double conversion and IGBT 6 kVA capacity in N+ N topology, 1 Phase input & 1 phase output, rack mountable (≤ 2U) with unity power factor and efficiency up to 95.5%		
3.2.2	Input Voltage Range: 176Vac ~ 288Vac, at full load 100Vac ~ 176Vac, linear derating 100Vac, at half load; Input Power factor ≥0.99, at full load; ≥0.98, at half load		
3.2.3	Output Voltage : 220Vac/230Vac/240Vac (Single phase output) ; rated power factor as 1, Crest factor - 3:1 ; Voltage harmonic distortion < 2% (linear load); < 5% (non-linear load)		
3.2.4	Frequency synchronization range : Rated frequency±3Hz. Configurable range: ±0.5Hz ~ ±5Hz Frequency track rate : 0.5Hz/s. Configurable range: 0.2/0.5/1Hz/s (single UPS), 0.2Hz/s (parallel system)		
3.2.5	Overload capacity for the UPS : At 25°C: 105% ~ 125%, 5min; 125% ~ 150%, 1min; 150%, 200ms		
3.2.6	Certification & Compliance : General and safety requirements - IEC/EN 62040-1 , EMC - IEC/EN 62040-2 , IEC/EN61000-3-12		
3.2.7	Surge protection for UPS : IEC/EN-61000-4-5, endurance level 4 (4kV) (live line to earth), level 3 (2kV) (during live lines); ANSI C62.41, 6kV/20hms		
3.2.8	UPS should be RoHS & energy star certified with IP20 Protection level . Noise level should be < 55dB		
3.2.9	Operating temperature for the UPS : 0°C ~ 50°C ; Relative humidity : 5%RH ~ 95%RH, non-condensing ; Altitude ≤3000m; derating when higher than 2000m		
3.2.10	UPS system should support battery backup of 30 minutes on full load. Batteries to be placed in external battery racks.		

3.3	Racks & Accessories		
3.3.1	Rack is 42 U 19" mounting type with 2100 (Height) x 800 (Width) x 1100 (Depth) with safe load carrying capacity of 1400 Kg on enclosure frame and 1000 Kg on 19" mounting angles		
3.3.2	Front Glass door for complete 42U height visibility and rear split steel door with stiffener and PU gasket for strength		
3.3.3	Cable entry provision from top & bottom both side of rack		
3.3.4	Cut outs with rubber grommet on top and bottom cover of rack for cable entry		
3.3.5	Vertical Cable manager on both LHS & RHS on rear side		
3.3.6	Thermally insulated cold aisle chamber		
3.3.7	Blanking panels to prevent air mixing		
3.3.8	Status based LED light to be provided on each rack		
3.3.9	Hybrid IPDU 02 nos per Rack(As per Specifications Given below)		
3.4	Safety & Security		
3.4.1	Access Control		
	The system deployed will be rack based access control system based on electronic Technology. The front rack doors should be operated with Biometric door access system and will operate on fail-safe principle through Biometric access control system. Rear doors should be operated with auto lock opening system. Should have provision for auto opening of Door in case of Emergency situations.		
3.4.2	Rodent Repellant System		
	Racks to be covered with rodent repellent system		
3.4.3	Fire detection & Suppression System		
	Rack to be covered with Fire alarm system		
	The system should have fire suppression unit mounted internally / externally on the rack .		
	The fire suppression agent should be NOVEC 1230 Gas as per NFPA 2001 guidelines		
3.5	Monitoring		

	Detailed Monitoring & Diagnostics thru Rack Data Unit ,1U rack mountable , with redundant power supplies & capable of single window monitoring of all the environmental parameters i.e IP based monitoring of temperature, humidity, water leak detection, smoke, etc through a single window dashboard.		
3.6	Electrical System (POD Device):		
	19" rack mountable Power Output Device with essential breakers to be mounted in the rack.		
3.7	OEM Credentials		
a	The critical components like Cooling unit , Rack, electronic door access, auto door opening system & Monitoring unit preferably from same & single OEM for better integration & service support .		
b	(DX) Rack based air conditioning unit using refrigerant R407C/R410A. Test certificate shall be submitted prior to shipment		
c	The OEM must have executed minimum 5 Modular/Smart Rack Data Centre infrastructure projects during the last 3 years from the of bid submission date.		

- **Hybrid iPDU :**

S. No.	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The input rating of the iPDU should be 3 phase, 32A, 400V. The input cable must be minimum 3-meter-long, and the input industrial plug should be IEC60309 for three phase Input and must be Splash proof IP44.		
2	iPDU should have min. 24 numbers of UL certified hybrid outlets which should be of hybrid nature which can be utilised as either C13 or C19 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords. The IPDU hybrid outlets should meet electrical compliance and should be UL certified.		

3	Monitoring parameters – The IPDU should have monitoring capability at the Strip level and Circuit/ Breaker monitoring.		
	Following monitoring parameter should be available at input level		
	1.) Voltage (V)		
	2.) Current (A)		
	3.) Power factor		
	4.) Active power (W/KW)		
	5.) Apparent power (VA/KVA)		
	6.) Energy consumption (kwh)		
	The metering accuracy should be +/- 1% compliant to ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements for strip level.		
5	IPDU should have 6 numbers 16A magnetic circuit breakers for overcurrent protection in three phase PDU		
6	The IPDU should have color coded outlets based on circuit color for easy identification of circuits for quick troubleshooting and ease in maintenance.		
7	The IPDU should support the daisy chain of minimum 40 units to reduce network port requirement and ensure continuous flow of data on network to monitoring tool/BMS/DCIM even a break in daisy chain occurs.		
8	Network communication – PDU should have two Network Ports. IPDU should support communication protocols including DHCP, HTTP, HTTPS, Ipv4, Ipv6, LDAP, NTP, RADIUS, RSTP, SSH, SMTP, SSL, SNMP (v1, v2, v3), Syslog and TACACS+. Communication module should be hot- swappable, so that it can be replaced without powering off the PDU.		
9	IPDU should support encryption via TLS1.3 for additional security.		
10	The IPDU should support an android or iOS app to read power data securely. Some mode of communication should be provided using which IPDU data can be accessed while user is inside the data centre and IOS/Android app should not use Bluetooth or Wi-Fi connectivity to prevent breach.		

11	IPDU should proactively monitor environmental conditions within the cabinet to ensure optimal operating conditions. IPDU must support temperature, humidity, airflow, dew point, door position and flood detection sensors.		
12	Each rack to be provided with 2 IPDUs and 2 combo sensors (Temp., humidity & Dew point).		
13	The IPDU should support grouping of minimum 40 rPDU and rPDU sensor in the interconnected array to create the aggregated measurements like total rack power, total row power average power, max and min power, maximum temperature, maximum humidity, minimum temperature, minimum humidity, average temperature, average humidity in the row without use of any additional software.		
14	The IPDU should be high temperature grade, operating temperature up to 60°C.		
15	The IPDU shall have rotatable display, to easily read the displayed values when PDU is mounted upside down, based on the site requirement.		
16	IPDU must support software-based mass firmware upgrades, backup and configuration.		
17	IPDU should have USB support for firmware upgrade, backup, restored device configuration or expand logging capacity via USB storage device.		
18	IPDU should have separate reset buttons for reset to factory defaults and separate button to reset IP only, if other configurations are not to be altered.		
19	PDU should support configuration of user defined thresholds, reports and email alerts and send it automatically to the configured users automatically on the scheduled time intervals.		
20	The IPDU should have approvals form RoHS, CE marked, EN55032 and 55024, IEC 60950-1.		
21	All the three phase PDU should have color coded alternate phase outlets for simplified circuit/phase balancing and cable management.		
21	PDU should support integration with Power Management Software/DCIM for providing periodical data of power consumption.		

22	The solution will support warranty period of minimum 3 years, which include firmware upgrades, technical support and RMA during the period		
23	OEM or Manufacturer should be ISO 9001: 2000, ISO 14001 , ISO/IEC 27001:2013 and ISO 45001 certified.		
24	OEM Service Support for Major Equipment's / OEM or Manufacturer should have its own service centers in the cities where this solution to be implemented.		

53. Non Smart Rack with Redundant IPDU

Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Front doors in Steel fully perforated curved steel		
Rear doors in steel dual split, fully perforated		
The rack should be powder coated to avoid rusting and damage.		
Vented top cover with cable entry provision		
Bottom Cable entry		
Fully reversible 19" mounting angles at front and rear		
Rear 19" mounting angles supplied as split pairs to allow easy adjustments for equipment of different depths.		
Side panels with Slam latches and Indents for improved strength and aesthetics		
Side panels 2000Hx1200D (set)		
Comfort handle with lock & Key		
Rear door mount Fans		
Cable management Duct with 1U Cable managers		
Earth conduit kit with Rail		
Captive hardware pack of 20 Secure Screws		

Component Shelf 720mm Depth - 2 Nos		
Baying Kits		
Racks should be with all requisite accessories and parts.		
2 numbers of Hybrid iPDU (as per annexure) Metered PDU with minimum 10 sockets each and power cord, with ability to monitor power consumption of individual servers and network equipment.		
Supply and installation/laying of all the required electrical cabling to the racks shall be carried out by the bidder as per standards. All accessories for successful installation of rack should be supplied by Bidder.		

54. LED Display

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Product type	LED		
Panel Technology	IPS		
Screen Size	65"		
Resolution	3840 x 2160		
Connectivity	HDMI, USB, Ethernet		
Design	Bezel-less/ Narrow		
Number of HDMI Ports	3		
Number of USB Ports	1		
Number of Ethernet Ports	1		
Speaker	10W x 2		
Operation Temperature	0°C to 40°C		
Power Supply	AC 100-240V~, 50/60Hz		

Smart Energy Saving	Yes		
Remote	Yes		
ACCESSORY	Basic: Remote Controller, Power Cord, QSG, Regulation Book, Phone to RS232C Gender Optional: Stand (ST-653T), Wall bracket(LSW350B), VESA Adapter(AM-B330S)		

GENERAL NOTE for all Active equipment(s) : Bidder shall supply required quantity of fiber patch chords (Single mode/ Multimode), patch chord as per site requirements. All accessories for successful installation in rack should be supplied by Bidder.

55. Heavy-duty workstation

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Processor	Intel 12th Generation Core i7 Processor or AMD Zen 3 Ryzen 7 series		
OS	Windows 10 Pro/11		
RAM	64GB, DDR4, 3200MHz		

Storage	512GB Solid State Drive (Boot) + 1TB 7200 RPM Hard Drive (Storage)		
Monitor	24" inch FHD IPS (1920 x 1080) Anti-Glare Narrow Border Infinity Touch/ Non-Touch Display		
Camera	FHD Camera		
Ethernet	Dual 1000BASE-T Ethernet Adapter		
Ports	1 HDMI / VGA, 1 Audio-in / out, 1 USB 2.0, 1 USB 3.0		
Keyboard	Standard Wired USB Keyboard (same OEM Make		
Mouse	Two button scrolling wired USB Optical Mouse (same OEM)		

56. Laptop

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Processor	11th Generation Intel® Core™ i7-1165G7 Processor (12MB Cache, up to 4.7 GHz)		
OS	Windows 10 Pro/11		
RAM	32GB, DDR4, 2666MHz		
Storage	512GB Solid State Drive (Boot) + 1TB 5400RPM Hard Drive (Storage)		

Monitor	14" inch FHD (1920 x 1080) Anti-Glare Narrow Border Infinity Touch/ Non-Touch Display		
Ethernet port	Ethernet port In built Ethernet card for LAN connectivity or external branded Ethernet RJ 45		
USB Ports	Ports USB 3, USB 2.0		
HDMI Port	Yes		
Wireless	802.11ax 2x2 Wi-Fi + Bluetooth 5.0		
Camera	FHD Camera		
Security	TPM 2.0		
Head phone Jack	Yes		
Microphone Jack	Yes		
Speakers	Yes		

57. Printer

Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
Type	All In One, office Jet		
Device Function	Print, Copy, Scan		
Print Type	Colour		
Minimum Speed per Minute as per ISO/IEC 24734 in A4 Size-Monochrome	25		
RAM	2GB		

Original Document Feeder Type	ADF, DADF/RADF, SPDF Or higher		
Scanning Feature Availability	Yes		
WiFi	Yes		
Duplexing Feature Availability	Yes		
Networking Feature Availability	Yes		
Compatible OS: Win 10, Win 7	Windows 10 Pro/11 ,Win7		

58. Privileged Access Manager

Privileged Access Manager	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
The Solution Should be On-Premise and hardware-based appliance and configurable in HA mode.		
Authentication Models		
· There should be a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc.		
· The solution should be agentless i.e. does not require to install any agent on target devices		
· The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection		
· The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.		
· The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server		

<ul style="list-style-type: none"> • The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism 		
<ul style="list-style-type: none"> • The solution should also provide local authentication and all the security features as per best standards. 		
<ul style="list-style-type: none"> • The solution should provide flexibility user/device wise for local authentication or enterprise authentication 		
<ul style="list-style-type: none"> • The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors. 		
<ul style="list-style-type: none"> • The solution should provide multi-domain feature whereby the entire operations can be carried out within a tenant or line of business. 		
<ul style="list-style-type: none"> • The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs 		
<ul style="list-style-type: none"> • The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple data center may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations 		
Password Management		
<ul style="list-style-type: none"> • The solution shall perform password change options which is parameter driven 		
<ul style="list-style-type: none"> • The solution should set password options every x days, months, years and compliance options via the use of a policy 		
<ul style="list-style-type: none"> • Ability to create exception policies for selected systems, applications and devices 		
<ul style="list-style-type: none"> • The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system. 		
<ul style="list-style-type: none"> • The solution enables an administrator to change a target account password to a random value based on a manual trigger or automatic schedule. 		
<ul style="list-style-type: none"> • Allow single baseline policy across all systems, applications and devices (e.g. one single update to enforce baseline policy 		
<ul style="list-style-type: none"> • The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand') 		
<ul style="list-style-type: none"> • Ability to generate 'One-time' passwords as an optional workflow 		
<ul style="list-style-type: none"> • Ability to send notifications via email or other delivery methods triggered by any type of activity 		

· Ability to send notification via email to the user requesting the password that checkout is complete		
· Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period		
· All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys		
· The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		
· The solution should have the ability to reconcile passwords manually, upon demand		
· The solution should automatically verify , notify and report all passwords which are not in sync with PIM		
· The solution should have the ability to automatically "checkout" after a specific time and "check-in" within a specified time		
· The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.		
· The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.		
· The solution should be able to control re-prints with adequate authorization		
· Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)		
· The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests.		
Access Management		
· The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end user		
· The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM		
· The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end user.		
· The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/), front-end database utilities on any combination of target account, group or target system and end-user		

<ul style="list-style-type: none"> • The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc. 		
<ul style="list-style-type: none"> • The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user 		
<ul style="list-style-type: none"> • The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user 		
<ul style="list-style-type: none"> • The solution can restrict user-specific entitlements of administrators individually or by group or role 		
<ul style="list-style-type: none"> • The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical. 		
<ul style="list-style-type: none"> • The solution can restrict target-account specific entitlements of end users individually or by group or role. 		
<ul style="list-style-type: none"> • The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired. 		
<ul style="list-style-type: none"> • The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time. 		
<ul style="list-style-type: none"> • System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH 		
Privileged Session Management and Log Management		
<ul style="list-style-type: none"> • The solution should be able to support an session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments 		
<ul style="list-style-type: none"> • The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh, sql+ 		
<ul style="list-style-type: none"> • The solution should be able to log/search text commands for all sessions of database even through the third party utilities 		
<ul style="list-style-type: none"> • The solution should be able to log/search based on text commands for all sessions 		
<ul style="list-style-type: none"> • The solutions should support option for enabling session based recording for all sessions on any combination of target account, group or target system and end-user. 		
<ul style="list-style-type: none"> • All logs created by the solution should be tamper proof and should have legal hold 		

<ul style="list-style-type: none"> · The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group 		
<ul style="list-style-type: none"> · The tool can restrict access to different reports by administrator, group or role. 		
<ul style="list-style-type: none"> · The tool generates reports in at least the following formats: HTML, CSV and PDF 		
<ul style="list-style-type: none"> · System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts 		
<ul style="list-style-type: none"> · The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats (non-editable and encrypted) preferably in any proprietary format. 		
<ul style="list-style-type: none"> · The session recording should be SMART to help jump to the right session through the text logs 		
<ul style="list-style-type: none"> · Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc. 		
<ul style="list-style-type: none"> · The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary 		
<ul style="list-style-type: none"> · The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording (Optional). All other commands will be included. 		
<ul style="list-style-type: none"> · The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution The proposed solution shall allow configuration at platform level to allow selective recording of specific device (Optional). 		
<ul style="list-style-type: none"> · The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables). It should have capability to support End point privilege management. 		
<ul style="list-style-type: none"> · The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity. 		
<ul style="list-style-type: none"> · The proposed system shall support full colour and resolution video recording. 		
<ul style="list-style-type: none"> · The proposed system shall support video session compression with no impact on video quality. 		
<ul style="list-style-type: none"> · The proposed solution should have offline vault for Break glass scenarios . 		
PIM Security		
<ul style="list-style-type: none"> · All communication between system components, including components residing on the same server should be encrypted. 		

<ul style="list-style-type: none"> · All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway) 		
<ul style="list-style-type: none"> · The Administrator user cannot see the data (passwords) that are controlled by the solution. 		
<ul style="list-style-type: none"> · Secured platform -main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.). 		
<ul style="list-style-type: none"> · Solution should be TLS1.2 and SHA-2 Compliant and can validate FIPS 140 -2 cryptography for data encryption. 		
<ul style="list-style-type: none"> · The solution should secure Solution should secure master data records, entitlement, policy data and other credentials in a non-modifiable storage device/process. 		
PIM Administration		
<ul style="list-style-type: none"> · There must be central administration web based console for administration, user and device management and having of feature to auto on-board them. 		
<ul style="list-style-type: none"> · The tool uses Active Directory/LDAP as an identity store for administrators and end users. 		
<ul style="list-style-type: none"> · The tool enables an administrator to define groups (or similar container objects) of administrators and end users. 		
<ul style="list-style-type: none"> · The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one super group. 		
<ul style="list-style-type: none"> · The tool enables an administrator to define a hierarchy of roles without limit. 		
<ul style="list-style-type: none"> · Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address. 		
<ul style="list-style-type: none"> · Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly 		
<ul style="list-style-type: none"> · Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.). 		
<ul style="list-style-type: none"> · All administrative task should be done LOB wise i.e. Line of Business Wise 		
Architecture		
<ul style="list-style-type: none"> · Support of multi-tier architecture where the database and application level is separated 		
<ul style="list-style-type: none"> · Scalable Architecture (Horizontally /Vertically) and not limited to restricted hardware/Software count. (Specified correctly if there is such limit) 		

· Solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.		
· Solution can support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.		
· Solution shall have options for backup or integration with existing backup solutions		
· Solution can handle loss of connectivity to the centralized password management solution automatically.		
· There should not be any requirement of change in existing network topology to control privilege session and can support distributed network architecture where different network segment can be controlled centrally.		
· Solution should support client based and browser based administrations.		
· Solution should preferably be an agentless and include password management and session recording features.		
· Solution must support parallel execution of password reset for multiple concurrent request.		
· Solution should support failover form single active instance to stand by instance without loss of any data.		
· Solution should support virtual server instance for management and installation if required.		
· Solution can support multiple instance with load balancer if required in future.		
· System should support for implemented in high availability mode		
· Solution should have capability to have direct connection with target device using secured gateway channel without compromising risky ports.		
· System has ability to integrate with enterprise authentication systems like ADS, LDAP, windows SSO, RADIUS etc.		
· Systems has ability to integrate BIOMETRIC Solution, Hardware/Software Tokens, Ticketing system, HSM (Hardware Security Module), Automation Software if any.		
SIEM Integration		
· Solution should be able to integrate with leading SIEM Solutions and or other performance monitoring applications to eliminate password hardcoding feature.		
Password Management		

<ul style="list-style-type: none"> • Solution should manage to protect and preferably eliminate privileged credentials in application, scripts or configuration files. 		
Discovery of Privilege Account		
<ul style="list-style-type: none"> • Solution should authenticate and trust the application requesting privilege password. 		
<ul style="list-style-type: none"> • Solution should be capable to discover privilege accounts on target system, manage user governance and can reconcile it. It can identify non built-in local (backdoor) admin or equivalent account. 		
<ul style="list-style-type: none"> • Solution should identify public/private SSH key, orphan key, and can ascertain its status. 		
-		
Notification of Alerts		
Solution should be able to generate alert through SMS/Email		
<ul style="list-style-type: none"> • For any critical PIM Events and able to send message 		
<ul style="list-style-type: none"> • For any change in Admin rights or configuration file 		
<ul style="list-style-type: none"> • On Other critical events based on customization 		
Dash-Board/Reports		
Solution should provide		
<ul style="list-style-type: none"> • Real time view of the activities of Administrators 		
<ul style="list-style-type: none"> • Reports based on defined frequency, on-demand 		
<ul style="list-style-type: none"> • Scheduled Reports like User Activity/Privileged account list/ activity logs 		
<ul style="list-style-type: none"> • System Administrator changes performed by PIM Admin 		
<ul style="list-style-type: none"> • Reports of password lockouts/checkout on system/password change report/Password status 		
<ul style="list-style-type: none"> • Other customised reports 		
<ul style="list-style-type: none"> • Other Audit Reports based by IT auditor's requirement 		
<ul style="list-style-type: none"> • Ability to replay actual session recording for any forensic analysis as and when required. 		
<ul style="list-style-type: none"> • Dashboard for viewing critical events and password polices. 		

Other Miscellaneous:		
· Credential management for privileged accounts of servers with different OS, databases and network devices		
· Delegation of access to privileged accounts		
· Controlled elevation of commands		
· Secrets management for applications, service and devices		
· Privileged task automation (PTA)		
· Remote privileged access for workforce and external users		
· Unified Central dashboard to monitor & manage all activities, accounts, policies and auditing		
· Approval workflows to automate the privileged escalation requests		
· Ability to monitor live sessions, and if required, capability to pause or terminate the session		
· Build reports for usage, audit, forensics, and regulatory compliance purposes.		
· Defined user activity should generate real-time email alerts, as well as block commands, lock, and terminate SSH sessions.		
· 'log off on disconnect' feature to ensure sensitive data is not exposed in subsequent RDP/SSH sessions.		
· Granular access control mechanism for Unix / Linux commands		
· Alerts on invoking unprivileged access and suspicious activity.		
· Ability to store the audit logs and recordings for 1 year and option backing up the logs using sftp or any other mechanism.		
· Solution sizing should be done to support 2000 Target systems and the licenses should be supplied on day 1 for 1500 Target systems.		
· Solution should be supplied with all the required hardware.		
· Solution should work in HA with active standby and audit logs should be mirrored across the Active / Standby systems.		
· OEM should be ISO 27001 certified.		
Support		
This application must support all type of devices including servers, storage routers, firewalls, switches etc placed within DC and DR.		
Licenses should be provided for a duration of 3 years.		
Sizing requirement:		

• The appliance should have storage capacity of more than 10 TB for retention of audit records and option to export the audit records over sftp / rsync for backup.		
• Number of Named Users - 50		
• Target Systems - 1500		

PART B

1. Data Center Infrastructure Management (DCIM), RF Id Based Rack Level Live Physical Asset Tracking & Heat Humidity Sensor Solution

S.No	Specifications for Data Center Infrastructure Management (DCIM), RF Id based Rack Level Live Physical Asset Tracking, Heat and Humidity Sensor based Solution	Marked/ Highlighted Cross Reference of Specification with reference page no. in bid.	Compliance (Yes/No)
1	<p>The DCIM may be pre-integrated with EMS solution from single OEM or the DCIM solution may be from different OEM than EMS OEM. It must be ensured that RF Id based Rack Level Live Physical Asset Tracking Solution (including its asset tags), Heat and Humidity Sensor based Solution (including its sensor tags) & DCIM should be from one single OEM.</p> <p>The Unified Data Center Infrastructure Management Solution should provide real-time visibility & access across all IT and facility resources including DC & DR .</p> <p>These resources comprise of :</p> <ul style="list-style-type: none"> i. Existing 32 RACKs at DC location installed & commissioned during phase-1 stage-1 of this project. ii. Non IT and IT equipment such as NEs and Servers being installed & commissioned at DC during the phase-1 stage-1 of this project. iii. New RACKs being installed & commissioned at DC and DR via this bid. iv. Non IT and IT equipment such as NEs and Servers to be installed & commissioned at DC and DR via this bid. 		

2	<p>It should be a comprehensive SSL 256 bit secure web based & an enterprise grade solution, consisting of all enterprise grade industry standard features. Bidder holds the responsibility to ensure the complete integration and testing of these modules before proposing an integrated solution in the bid.</p> <p>The solution should include a RFID based Rack level live physical asset tracking and monitoring solution(RLPAT). It should also include a Heat and Humidity sensor solution . The RF Id based Rack level live physical asset tracking solution and Heat and Humidity sensor solutions may be separate modules in themselves, but must be well integrated with DCIM solution as per specs & scope of work. These two modules must also be integrated with proposed EMS solution in this bid.</p> <p>RF based Physical Asset Tags and Humidity and Temperature sensor Tags should also be provided for the existing racks supplied in phase 1 at DC besides the equipment supplied & installed in this bid.</p> <p>It may be noted that RFID based live asset tracking is not required at Remote Locations, the assets / inventory should be tracked & audited manually at these locations by the system integrator as a scope of work. The complete solution should have a perpetual license.</p>		
3	<p>The solution should be able to detect, collect, register and manage information on infrastructure elements related to Power, Temperature , Cooling , Rack space, rackPDUs , Assets tags of data center. It shall show available power, available space, heating and cooling on floors in racks, and network ports and power connectors on the UI/dashboards readily, depending upon the interfaces. There will be an existing BMS system, bidder must scope & plan to integrate with BMS (if the access/permissions are provided) for any of the relevant data for any of such systems.</p>		

4	<p>Solution should provide mapping of assets on the state level , city level, building level , floor level rack level etc. so as to pinpoint the asset location and area. In case the solution has any geo-maps, the solution should not connect with Internet for this or any of such feature, the maps must be in-built. The solution should support 2D and 3D based visualization for Areas, Buildings, Floors, Rack Aisles, Racks, equipment level views. These views should be able to show the interfaces of all device types, storage, I/Os. The solution should be bundled(in-built) with Symbols library for OEM icons, Device maps, and Item shapes and Icons etc. Should have capability to upgrade this symbol's library as well. It should integrate with EMS in a way so as to present the alarms per equipment level in this visualization view. Overall, the solution will not have privileges to connect to internet, it must support any updates via non Internet based mechanisms.</p>		
5	<p>The solution should support the</p> <ol style="list-style-type: none"> i. counting of Rack Aisles, Rackspace etc. ii. Power Consumption Monitoring for Elements in racks of DC and DR iii. Display of Heatmap view 		
6	<ol style="list-style-type: none"> a. The solution design and deployment architecture should meet the availability requirements ensuring that the deployed solution should be distributed or has a load balanced implementation of application(s) to ensure that availability of services is not compromised at any failure instance. <ul style="list-style-type: none"> • b. The complete solution should be provided in High Availability mode . There should be seamless automatic successful switchover/handover (in case of failure) between the two instances. The respective HA mode instances of applications/modules should execute at different physical servers. The servers should be of industry standard and data center compatible. Each instance should be able to manage & monitor complete infrastructure at DC and DR. <ul style="list-style-type: none"> • c. SI must ensure the automatic sync of all relevant data amongst the different data bases of the instances. There shouldn't be any data loss during or after completion of sync. <ul style="list-style-type: none"> • d. The SI must budget to provide the relevant hardware / software (if any) which can sync DCIM & its module's data from DC to DR and vice versa (DR to DC sync is 		

	<p>applicable in special cases when DC went down and comes back). The software must only sync the delta (i.e. changed part) everytime to maintain whole database sync.</p> <p>e. It must be noted that in case the HA is provided within two instances running on different physical servers at DC</p> <ul style="list-style-type: none"> • SI must ensure to provide another third instance at DR , which will remain passive until complete DC is down and/or as per any other defined scenario. • When the link between DC and DR goes down & DC's instance is monitoring - managing the DC's infra, the instance at DR must monitor - manage DR infrastructure. The data (such as alarms etc.) must be synced with DC instance , when DC-DR link comes back. Also on such occasions/scenarios, whenever the DC and DR instance are running actively at same point of time, solution should not require any additional licenses. Sufficient licenses for the solution should be provisioned to handle such scenarios i.e. ensuring DC and DR instance can run without the need for any extra license. • SI must create Standard operating procedure document for replicating the data (from all of the supplied modules) from DC to DR on regular basis with a periodicity allowed to be defined (between 30min to 5 days). 		
7	Solution should connect and integrate with the Facility (Non-IT), IT infrastructure & Internet of Things(IoT) based systems in the same unified platform. The UI should remain unified for operators. Should be able to show faults/alarms from IT/IoT systems added to the platform.		
8	It should get integrated with EMS (proposed in this bid) for Alarms/Events, Change Management, IT helpdesk/Service desk (for any requests/authorizations) etc.		
10	The system shall have visual capability of 3D color-coded, floor map overlays, power, cooling, and capacity data, drilldown from floor map view to contents inside cabinets, thermal real time data.		
11	The system shall support preconfigured chart widgets, performance graphs, filters.		
12	The system shall allow to analyze KPIs and gain data center business insights from chart widgets with drilldowns across multiple dashboards that address most common reporting needs.		
13	The system shall have drilldown capability allows easy access to the data that drives charts.		

14	The system should be a RBAC (Role-based Access Control) based system with fine control over access and restrictions on monitored objects, groups, system elements. The UI should support and provision the operators to configure the settings. The system should be ready for AAA / LDAP based integration for RBAC. Bidder must do the AAA / LDAP integration as a part of scope of work for achieving these requirements.		
15	The system shall allow to track detailed information on data center IT equipment.		
16	The system shall allow to quickly search , locate & help to map server(s), network, and storage equipment etc. . It must provide various search / advanced search and filtering mechanism/criteria's . It should also allow to reserve the capacity by allowing to enter parameters such as RU height & Rack, no. of data connections and power connections etc. while reserving a capacity. It should be able to show reports about the reserved capacities.		
17	The system shall have pre-configured and pre-integrated dashboards views for the DCIM, & Operations Management System. The operators should be able to browse seamlessly across the platform.		
18	The system should allow to take intelligent decisions help in efficient data processing and data analysis		
19	The system shall have pre-configured dashboards display charts by category such as : Overall health, Overview, Custom Health Parameters, What-If, Inventory, Space, Power, Cooling, Connectivity, Change, Tabular Reports.		
20	The system shall have feature to visualize floor plan drawings and rack views in real time on the Dashboard.		
21	The system shall easily show real-time capacity, consumption for all the datacenter physical infrastructure on the Dashboard.		
22	The system shall have rich filtering allows quick search by several asset parameters.		
23	Apart from the trending feature , overall System proposed shall support Root-Cause Analysis so as to Isolate and pinpoint the problem area before it impacts the overall DC operations & business continuity while suppressing down the unwanted events.		

24	The search-locate-map option should also help to identify , vacant spaces in any of the racks in the datacenter, for insertion of newer servers/networking devices etc.		
25	Integration of Solution with Helpdesk and EMS : Whenever a fault arises in the monitored/managed infrastructure/ or its own solution, a ticket should automatically get logged as an incident in the service desk. The Alarm/Fault should be visible into the Integrated EMS system being proposed by SI in this bid. As a process, the ticket should be assigned with predefined/preconfigured SLAs to the concern team/team members.		
26	The system should help in optimizing power usage vs cooling on racks. Should also be able to determine the optimum placement of new equipment on the racks. Should be able to identify and calculate Stranded capacity i.e installed capacity (cooling, power, space) which can not be used to support the critical load.		
27	Should allow to effectively monitor the Power consumption of the infra, subject to the permission granted/availability of same interfaces for integration of DCIM/EMS with iPDUs installed (as iPDUs supply would not be the scope of work of this bid). Though upon permission, Bidder must provide integration with all iPDUs , RACK PDUs (Socket Level / Strip Level) . Also, should be able to monitor/manage per device level power failures as alarms (provided that the rack level PDUs allow the monitoring and / or management).		
28	Solution should provide a real look and feel of the layouts & equipment exactly as they are placed in the racks or on the floor. This must be shown on the exact floor and building layout .		
29	The client Web browser GUI shall provide a comprehensive user interface. It shall be constructed to function as an application and provide a complete and intuitive mouse- or menu-driven interface. It shall be possible to navigate through the system using a Web browser. The Web browser GUI shall (as a minimum) provide a navigation menu for navigation, and a pane for display of graphics, alarms/events, active graphic setpoint controls, configuration menus for operator access, analytics and reporting actions for events. All system graphics are to be HTML 5 compatible. The GUI shall atleast support browsers as : Microsoft Edge , Google Chrome , Mozilla Firefox etc.		

30	The Web browser GUI shall make extensive use of color in the user interface to communicate status information about the equipment being monitored.		
31	Equipment view - The equipment view shall show the status of applicable equipment such as rack, rPDU and so on. The view must allow users to drill down into equipment pages to view alarms and equipment information in full detail, including individual status of all associated device points.		
32	Floorplan views must provide geographical navigation and are flexible to show local data center specific views of site/location hierarchy. Components of the floorplan view must include: <ul style="list-style-type: none"> • Ability to import image to match level of hierarchy being viewed (map, data center, etc.) • Add groups, devices, racks, points, labels, or other devices to the floorplan view. • Ability to add a heatmap view, capable of showing hot spots and cold spots for environmental or power data • Visualization of alarms • When racks are added, a dropdown view selector to allow : alarm status, free front/rear rack U space, max contiguous front/rear rack U space, max rack temp, max rack kW load percent, total rack kW, heatmap view etc. 		
33	The user must be able to create, edit and add boards, dashboards and floorplan views		
34	Graphics shall show each piece of equipment monitored or controlled at : <ul style="list-style-type: none"> • Each building (DC/DR), • Each floor , • Each room , • Each rack , etc. 		
35	Events and alarms associated with a specific system, area or equipment shall be displayed on the main view and/or within an embedded alarm console. The solution must have native capability to show alarm on all connected devices. Users must be able to drill down through views to locate alarm sources. The alarm should be accessible from the device level. Multiple configurable severity levels for Alarms must be supported. System should support separate Rule Engine based alarms apart from the generic threshold(min, max and average values).		
36	The alarms generated in DCIM for the components should also be reflected in the EMS system.		
37	The user shall be able to view events across the system. Depending on access level, it should also be able to manage the event through acknowledgements, deletions, sorting rules and viewing alarm notes.		

38	<p>The system should support following two methods for third party integrations i. REST APIs (PUSH & PULL methods) ii. SNMP Trap Forwarding In case required bidder must be ready to perform an integration w.r.t Generated Log File (used for writing alarms / events) to achieve the overall functionality.</p>		
39	<p>Role based access / User Management</p> <ul style="list-style-type: none"> • Permissions: The Permissions field allows administrators to set access level for different users. Permissions should be role based permissions include options such as : <ul style="list-style-type: none"> o Read/Write: Full read access and full write access to the entire system. o Read Only: Full read access but no writes or changes may be done. o Read/Acknowledge: Full read but no write or changes may be done, except to alarm database for acknowledging alarms. System owner shall have the ability to assign combinations of roles and privileges to users that define access levels. The UI should support and provision the operators to configure the settings. The system provide a LDAP based integration while configuring users for Role based access. 		
40	<p>Audit History: A log shall record operator activities and some system level activities per user, such as configuration changes ,etc.</p>		
41	<p>Histories/Trending: Histories shall be user-configurable and displayed via GUI. Trends shall comprise native points, along with calculated points (collections of point data). A trend log's properties shall be editable within the GUI. The operator shall have the ability to view trends with a time series line chart by using the history database or by selecting a specific point within the GUI. The line chart must be exportable within the pop-up window to Microsoft Excel and able to be saved as a visualization to be used within the Analytics tool. Historical records shall be saved to match the "configurable" user-defined polling interval per device. Each trended point shall have the ability to be trended at a unique interval as specified by the user.</p>		

42	<p>IT Assets: The solution includes an asset database. IT Assets are representations of a physical rack assets that will be associated to IT Racks within the software. These assets are created within a dedicated assets feature. The assets feature contains a detailed list view of assets. The asset feature shall provide the following capabilities:</p> <ul style="list-style-type: none"> • Asset database which is sortable, filterable and searchable by key asset data • Add assets – manually or via CSV import • Edit assets individually or by group • Support of assets within assets (blade server enclosures, as an example) • Export & import of existing asset database • Ability to assign IT assets to IT racks • Asset tab within the Rack View to visually display IT assets within each IT rack 		
43	<p>Maintenance: The solution must provide users with a feature to manage device maintenance events. This feature will silence all alarms on specific equipment or multiple pieces of equipment for the duration of the maintenance event.</p> <ul style="list-style-type: none"> • Users must be able to place a device into maintenance mode instantly or schedule maintenance within the interface, for single or multiple grouped devices at a time. • Users have the option to receive email notification for the start and end of maintenance events. • Maintenance events must include start and end dates, devices and task descriptions. • Users must be able to view maintenance history. • The solution shall allow users to add, edit and delete maintenance tasks. Events that have completed cannot be deleted. 		
44	<p>Vendor must integrate DCIM solution & its modules with proposed EMS , Change Management , IT Helpdesk solution under this project. The bidder may integrate or also have to integrate this solution with other necessary (proposed) modules as desired to accomplish the required functionality.</p> <p>Bidder must also ensure that all the hardware of various different OEMs proposed in this solution by the bidder must be managed, monitored by the proposed DCIM+EMS solution. The proposed solution should be able to show the alarms from all sub-system & system components planned to be supplied in this bid including Phase-I and other bids referred in this tender. In general solution should be OEM agnostic & should by default support integration with major OEMs of Network and server equipment and natively support SNMPv3 for other devices.</p>		

	Humidity and Temperature sensor Solution & RLPAT Solution		
1	<p>Humidity and Temperature sensor tags are required which need to be mounted on each RACK placed at DC and DR only. The sensor should be able to provide both temperature and humidity from a single sensing tag and not two different devices. The sensors should stick to the RACK. Three sensors per RACK , with two in front and one at the back are required. Actual location on the RACK will be confirmed during Installation. The sensors must be operating in free ISM unlicensed RF Frequency bands . The solution shouldn't use 2.4/5Ghz bands (Wi-Fi/Bluetooth) instead use SubGhz bands. For completeness of requirements & efficient solution design, the solution may use the same Communication Gateway device (Proposed with RLPAT Solution) . The same Communication Gateway device shall be configured and integrate with Humidity and Temperature sensor tags and Asset Tags (supplied with RLPAT solution) in a Star Topology. The communication Gateway device may further connect with EMS/DCIM over SNMP/REST API or other possible mechanisms for accomplishing the requirements. The exchange of data amongst these devices should be in an encrypted form.</p>		
2	<p>The Humidity and Temperature sensor software Solution should be able to manage and monitor the Humidity and Temperature sensor tags, should be able to work as a standalone solution as well as should get integrated with DCIM to provide completeness of DCIM solution & scope of work. It should be a web based solution deployable as a standalone on a hardware or on a VM.</p>		

3	<p>Proposed sensors must allow in maintaining the environment within threshold defined via configuration at EMS/DCIM. The Humidity and Temperature sensor Solution should get integrated with DCIM/EMS solution . Overall these sensors should help the DCIM/ EMS in bringing the floor's heatmap view / each RACK wise heat view . The alarms generated via the sensor hardware supplied should be visible at DCIM and EMS solution supplied. The data(generated/configured) related to temperature & Humidity should be supplied to both EMS and DCIM e.g. the temperature data should be used at DCIM for the purposes of generating heat maps (visualization) etc . This is to note that this data (both temp and humidity) will also be required at EMS to generate any alarms such as whenever temperature / humidity goes beyond a configured threshold. Humidity and Temperature sensor Tags should also be provided for the existing racks supplied in phase-1 at DC . No Humidity and Temperature sensor Tags are required at remote locations.</p>		
4	<p>After integration with DCIM, the Solution should allow proactive identification of potential areas which may need attention (including cooling, power, storage, temperature etc.) .</p>		
5	<p>Real time heat & humidity measurement for equipment's on the racks should reflect on the central dashboard of DCIM.</p>		
6	<p>Sensors should not be larger than 35mm x 55mm x 8mm without enclosure and a should not exceed 76mm x 40mm x10mm with enclosure . Total weight of an enclosure should not exceed 75gms . The enclosure must be stuck on Rack using VHB Tapes . The enclosure must be Tough, impact resistant and temperature stable.</p>		
7	<p>Sensors should have accuracy of +/- 1degree Celsius and +/- 3 for relative humidity . They should be operatable within -20 °C to +70 °C & Operating Humidity levels < 95% RH non-condensing .</p>		
8	<p>Proposed solution must have an inbuilt feature to support multiple internal departments by mapping them against tenant ID, thus it should provide information regarding power used, capacity used by a tenant.</p>		
9	<p>The system should be a RBAC (Role-based Access Control) based system with fine control over access and restrictions on monitored objects, groups, system elements.</p>		

10	The system should be integrated with IT Helpdesk solution proposed by the SI via the DCIM or directly.		
11	<p>Solution should provide Rack level Physical IT Asset Tracking to optimize and keep a check on Datacenter IT inventory Tracking and audits. The software solution supplied to manage and monitor the Rack level Physical IT Assets Tracking should be able to work as a standalone solution as well & should get integrated with DCIM.</p> <p>It should be a webbased solution deployable as a standalone on a hardware or on a VM. The solution should be integrated with proposed EMS and IT Helpdesk solution by the SI via the DCIM or directly.</p>		
12	RLPAT Solution should be able to collect the information of IT assets and upload to a central database server provided. Near Real time monitoring of the assets location up to rack level by addition of tracking via asset tags so as to notify / alert the user(s) if an asset is added, moved, removed in an authorized or unauthorized manner. For completeness & compactness of the solution, the Live Asset Tracker are also required to be integrated with Communication Gateway to send the information to EMS/DCIM. They should use encrypted communication techniques for communication with Gateway		
13	Communication mechanism in RLPAT Solution should be wireless in nature & working on RF frequency (Unlicensed Band). The solution shouldn't use 2.4/5Ghz bands (Wi-Fi/ Bluetooth) and instead use SubGhz bands. This will be responsibility of the bidder that frequencies used in this solution should not interfere with any of the supplied equipment frequency or hamper any of their operations.		
14	RLPAT Solution's Asset Tag form factor & mounting - Form factor of asset tags should be small enough to be able to easily attach to a IT asset but it should also be noticeable to naked eye. Should not be more than 76mm x 40mm x10mm with enclosure No cables and wiring should run between asset tag to any hardware or RF / Controllers gateways. The Asset Solution should support OTA (Over the Air) upgrade of its components . The tags should be tough, impact resistant and temperature stable .		
15	RLPAT Solution's Asset tag & Heat and Humidity Sensor's battery Life - their battery should have Operational Life for atleast 3 years from date of acceptance of the solution. In case the battery life of tag is less than 3 years, SI shall provide the battery replacements until 3 years (from the date of acceptance) duration for each of the supplied tags .		

	The SI needs to also budget for a mandatorily replacement of battery (as a preventative maintenance of all asset tags with fresh battery in the last quarter of 3 rd year of O&M .		
16	RLPAT Solution's Asset tag Features - Should be able to alert in real time, if an unauthorized movement of asset is made or an asset falls or there is an attempt to remove or forceful removal of tag from asset or has a low battery. The solution must be an integrated solution with IT helpdesk, Change Management, DCIM etc., so as e.g. movement of asset can be authorized change request, whose time taken for a change may be tracked via the Helpdesk manager.		
17	RLPAT Solution's Alarms & Notification from the Asset Solution- Solution should be able to provide real Time alarm & event notification. Should be able to Generate Alert in atleast the following conditions: Addition & removal of Asset , movement of Asset from a RACK, Cage area, Store Room, FLOOR & DC/DR , Falling of an asset or there is an attempt to remove asset or a forceful removal of tag from asset or if an asset tag has a low battery & needs battery replacement or Out-of Warranty Alarm of the asset . Accordingly to the locations defined (such as RACK, Cage area, Store Room, Floor , DC,DR etc.) bidder may ascertain & accordingly include the number of Communication Gateways required)		
18	RLPAT Solution's Built in Local Indicator on Tags - All tags should have in-built indicators to reflect working status		
19	RLPAT Solution's Asset solution should support TLS & SSL, adheres to FIPS , access is protected through username & password. The OEM needs to provide an undertaking for FIPS adherence.		
20	RLPAT Solution's should have RoHS Certification		
21	RLPAT Solution's should have Capability -Locate IT asset accurately with Rack Level Accuracy		
22	RLPAT Solution's Battery in Asset tags must also be replaceable in nature & Tags should be reconfigurable/re-writeable		
23	RLPAT Solution's Asset solution should have Scalability - System should support minimum of 5000 tags in an area of 30,000 sqft.		
24	Assets Tags in RLPAT Solution should have a 2D barcode to allow ease of configuration or physical audits . Supplied Handheld Tag readers should be able to read , configure these 2D barcodes and save the information into the system about the asset if required. It should be		

	<p>compatible and integrated with the solution. It should have at minimum following communication interfaces, 4G LTE, WLAN , Bluetooth, NFC . It should have Environment specs with IP65 compliant and atleast 1.5mtrs Drop tested. It should have a minimum of 7000mAH battery & atleast 3GB RAM with 32GB Flash .</p> <p>The bidder is also required to provide two numbers of compatible 2D barcode / QR code printer along with consumables (Cartridge, DK Rolls stick able labels etc.)for 3 years duration. The Printer should have atleast 300dpi printing resolution, should have WLAN, RS232 and USB interfaces. Should support DK Rolls (DK die cut labels / DK Continuous Tape).</p>		
25	<p>RLPAT Solution's Integration - Should integrate with DCIM, EMS, Helpdesk/Service Management etc. modules of the system for various of its features such as authorization process of movement of an asset, raising alarms for unauthorized access/movement / tracking the assets .</p> <p>If an instruction is given to system to find an asset, it should be possible to locate that asset and give a beep sound locally on tag. e.g. If there was a request to move an asset from a RACK To another RACK in the IT Helpdesk system , this will be tracked via a ticket/service desk ticket. Any change needs to undergo via change management workflow , which means this request will be reviewed and approved by different users. Upon approvals a change becomes an authorized change. Similarly, if there is an alarm that arises in RF based physical asset system due to movement of an asset, this alarm must be sent to EMS. An alarm in EMS will auto raise a ticket in IT helpdesk (based on certain criteria) . The ticket may be closed by a user by referring / adding remarks to the ticket id w.r.t a ticket generated for authorized movement of asset as above. The alarm may be also acknowledged with this ticket id. The bidder needs to create such processes and perform similar integrations</p> <p>Data Integration - proposed solution should be able to route the data to DCIM/EMS by forwarding SNMP traps e.g. Alarm generated via an unauthorized movement of asset should be sent to EMS or any other alarm generated w.r.t Asset Management Functionality should be seen in EMS.</p>		
26	<p>RLPAT Solution's Inventory Management module should be able to manage assets inventory as individual or bulk items, set re-order levels and amounts and keep a history of transactions. Able to provide ability to account for assets and components in inventory and facilitates maintaining appropriate levels of stock .</p>		
27	<p>RLPAT Solution's Inventory management module should record OEM, Make, Model, Serial Number, Contract Details, Maintenance Details and link/maintain it in DB to each asset. User should be allowed to search the records/inventory based on any of fields / attributes .</p>		

28	The system should allow to generate the reports containing inventory details as mentioned above and including the other details such as current assigned IP, device type, device name, location , RACK etc.		
29	Asset record detail: Provide a general tab that stores specific information about the device depending on the device type.		
30	Provide a Components tab that stores sub-components information of the asset, E.g. ID, Serial Number, Licenses, Version, Status, Category, Type, Item, etc. and also should support in SLA management , assist in a Help Desk call.		
31	Provide a tab that stores information about different types of contracts and helps in Support, Warranty, Software, Maintenance , SLA, EoL, EoS etc.		
32	Provide a People tab / column that stores custom fields per asset such as individuals or groups who are owners and users of the asset.		
33	Should be able to provide the asset's inventory details along with details such as location, rack, IP details (where ever applicable). It should support both IPv4 and IPv6 stack.		
34	Deployment Mode of the overall Solution: The DCIM , RLPAT software module , Heat Humidity Module / Application(s) provided should be capable to be deployed on physical server and/or on virtual servers. They should all run in HA mode .		
35	Updating of Patches, Bug Fixes within support period, upgradation of version during the support period is the responsibility of the SI. SI must ensure to update the patches or provision the upgrades via the non-internet modes i.e. by following local update/upgrade mechanisms using HDDs/USBs .		
36	In case the solution consists of separate independent modules or as a single solution , each of them or the overall solution should be capable to run on Linux or Windows or on their VM . The solution with all modules, must run in HA mode in either case.		
37	<p>The proposed solution should include hardware(s) and software(s) (including web application stack, database, any servers, any other relevant software etc. required for accomplishing the scope of work and requirements) with operating system(s). Bidders must keep in mind the future and scalability of requirements before deciding for a hardware configuration.</p> <ul style="list-style-type: none"> • Also, the sizing of the computing in the proposed hardware should be sufficient enough to cater to futuristic projection of IT & Non-IT equipment mentioned in this bid. • Moreover, the specifications of the proposed computing hardware must be chosen so as to ensure that only 60% of the CPU and RAM are utilized at any point in time. In case 		

	<p>a higher CPU / RAM than this defined threshold is observed for more than 60 seconds, the bidder shall upgrade/replace (with higher specifications) the hardware within 31 working days. Otherwise, equipment will be considered down and SLA/Penalty will be applicable.</p> <ul style="list-style-type: none"> • The specifications of the proposed computing hardware and overall solution must be sufficient enough to handle infrastructure of such 3 additional data centres. • The proposed hardware must be scalable in future. <p>The proposed solutions/Modules for the sought requirements should be able to run on latest versions of Microsoft windows and Linux operating systems. All the updates and upgrades of the proposed solutions/Modules must also be supported on the upgraded / updated versions of OS during the entire contract period. The bidder also needs to provide the relevant software to ensure security of the provided hardware, software/ system.</p> <p>In case of any updates/upgrades of base OS, the supplied solution(s) must be updated/upgraded free of cost during the entire contract period. Also any bug fixes within support period must be supported.</p>		
38	The proposed solution should provide a secured single sign-on and unified console for seamless cross-functional navigation for all functions of components/modules offered across multiple areas of monitoring & management.		
39	Proposed solution should provide current and historical reports for various statistics monitored. The solution must also allow for generation of customized reports in addition to default reports as per templates. System should be able to generate the current alarm/assets etc. reports for entire inventory or per device basis. Reports should allowed to be generated for the historical data with custom time period. Should allow sending out(emailing) of all types of reports on custom schedule such as daily, weekly, monthly basis etc. Reports should be allowed to be generated in various templates such as excel, csv, pdf etc.		
40	The SI is required to provide a clean VAPT report of the complete solution at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution . Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done , upon any major upgrade in solution or solution's respective modules.		
41	There should be only one single OEM of Data Center Infrastructure Management (DCIM), RLPAT, including its asset tags & Heat and Humidity Sensor based Solution including its sensor tags.		

42	OEM should be ISO 9001, ISO 14001,ISO 27001 certified.		
----	--	--	--

2. EMS Solution

S.No	Specifications for Enterprise Management Solution(EMS) , Asset Manager , IT Helpdesk Manager , Change Management, Configuration Management , IPAM	Marked/ Highlighted Cross Reference of Specification with reference page no. in bid.	Compliance (Yes/No)
	General Requirements		
1	<p>It should be a comprehensive SSL 256 bit secure web based IPv4 and IPv6 compliant solution, consisting of all standard features/modules of Enterprise Management Solution (EMS) such as fault management, performance management, configuration management, event management, an IT helpdesk/service desk to perform SLA management , Configuration Management Database(CMDB) ,incident, problem, document, schedule, holiday, asset management and has a inbuilt syslog server / capability to integrate a syslog server ,so as to act as a sysLog aggregator, EMS solution (including its various modules) should provide traffic analysis , service management & their respective functionality on all the Non IT and IT (network and server) infrastructure procured and/or deployed at following different physical locations:</p> <p>i. 32 RACKs at DC location & its 15 remote locations including the Non IT and IT equipment such as NEs and Servers at these locations from the phase-1 stage-1 of this project.</p> <p>ii. New RACKs being installed & commissioned at DC, DR and its remote locations including the Non IT and IT equipment such as NEs and Servers to be installed and commissioned at these locations via this bid.</p> <p>iii. IT Equipment being purchased via the bid “GEM/2022/B/2183782” titled as “Selection of System Integrator For Setting up of ICT (Security) Infrastructure at 18 Remote Sites”.</p> <p>The solution in general should be able to manage/ control/ configure/ integrate/ view alarms from all of infrastructure from above equipment commissioned at these sites.</p> <p>The complete solution should have a perpetual license.</p>		

2	<p>The proposed EMS solution can be from a single OEM or final EMS solution with IPAM including Switch Port Management may be an integration of OEMs to fulfill the sought requirements, in other words, EMS solution and all modules (e.g. Configuration Management , network monitoring, server monitoring, asset management, IT Helpdesk , Change Management etc.) must be from a single OEM where as the IPAM Solution may be from a different OEM to fulfill the sought requirements & functionality. Bidder holds the responsibility to ensure of testing the functionality of these components/modules before proposing a solution in the bid.</p> <p>The proposed solution should be able to manage and monitor all the devices mentioned & planned as per requirements and scope of project.</p> <p>Solution OEM(s) should have a development/development support center in India to facilitate quick issue / bug resolution/ any custom requests and upgrades. EMS Solution should be a GUI based support portal with all features mentioned in EMS Specifications</p>		
---	--	--	--

3	<p>Proposed solution must provide role based access for each user / user groups. The access & privileges of users/user groups should be possible on per module/application basis . The users/user groups access should be possible on features within the modules/applications on Read only or Read-Write basis per feature.</p> <p>The role based read/read-write privileged user /user groups should also be possible for various solution module(s) sought , device level groups(network groups, server groups etc.)</p> <p>The RBAC (Role-based Access Control) system with fine control over access and restrictions on system elements/modules/functionality should be supported for all the supplied modules/applications. The module/application UI should support in provisioning the operators to configure these settings via an administrative login. Integration : The system should be ready for AAA and AD based integration to support these features. Bidder must do the AAA and LDAP integration as a part of scope of work for achieving this role based requirements and AAA integration for authentication between EMS and Network devices must be performed prior to acceptance.</p> <p>The users should have same login credentials to access these various modules while navigating across the solution. The access to various modules should be dependent upon privileges defined per user per module.</p>		
4	<p>The proposed solution should include hardware(s) and software(s) (including web application stack, database , any servers etc. required for accomplishing the scope of work and requirements) with operating system(s) . Bidders must keep in mind the future and scalability of requirements before deciding for a hardware configuration.</p> <ul style="list-style-type: none"> • Also, the sizing of the computing in the proposed hardware should be sufficient enough to cater to futuristic projection of IT/Non-IT equipment mentioned in this bid. • Moreover, the specifications of the proposed computing hardware must be chosen so as to ensure that only 60% of the CPU and RAM are utilized at any point in time. In case a higher CPU / RAM than this defined threshold is observed for more than 60 seconds, the bidder shall upgrade/replace(with higher specifications) the hardware within 31 working days. Otherwise, equipment will be considered down and SLA/Penalty will be applicable. 		

	<ul style="list-style-type: none"> • The specifications of the proposed computing hardware and overall solution must be sufficient enough to handle infrastructure of such 3 additional data centres. • The proposed hardware must be scalable in future. <p>The application should be 64-Bit Application and run on 64-bit architecture. However, it may be noted by bidder before proposing the solution that no server or any other hardware is allowed to kept at remote locations for monitoring or management i.e. w.r.t EMS.</p>		
5	<p>The overall solution should be provided in High Availability mode . There should be seamless automatic successful switchover/handover (in failure cases) between the two instances. The respective HA mode instances of applications / modules should execute at different physical servers. The servers should be of industry standard and data center compatible. Each instance should be able to manage & monitor complete infrastructure at DC ,DR & Remote Locations.</p> <p>SI must ensure the automatic sync of all relevant data amongst the different data bases of the instances. There shouldn't be any data loss during or after completion of sync.</p> <p>The SI must budget to provide the relevant hardware / software (if any) which can sync EMS & its module's data from DC to DR and vice versa (DR to DC sync is applicable in special cases when DC went down and comes back). The software must only sync the delta (i.e. changed part) everytime to maintain whole database sync.</p> <p>It must be noted that in case the HA is provided within two instances running on different physical servers at DC</p> <ul style="list-style-type: none"> • SI must ensure to provide another third instance at DR, which may remain passive until complete DC is down and/or as per any other defined scenario. • When the link between DC and DR goes down & DC instance is still in active state monitoring DC equipment, the instance at DR must monitor and manage DR infrastructure and remote locations. The data (such as alarms etc.) received at DR must be synced with DC instance, when DC-DR link comes back. Also on such occasions, whenever the DC and DR instance are running actively at same point of time, should not require any additional licenses. Sufficient licenses for the solution should be provisioned to handle such scenarios i.e. ensuring DC and DR instance can run without the need for any extra license. • SI must create Standard operating procedure document for replicating the data (from all of the supplied modules) from DC to DR on regular basis with a periodicity allowed to be defined (between 30min to 5 days). 		

	Note : Each instance of the application provided e.g. One instance of the EMS solution while working in HA mode (as an example) should be able to manage and monitor the 100% of the infrastructure (mentioned above i.e. all Infra at DC , DR & remote locations and already existing phase-1 infra and its remote locations, etc. as per scope of work) irrespective of its location of execution on a physical server .		
6	The proposed software and hardware should be scalable to accommodate network growth of upto 10,000 IT Devices (including 4000 Networking Devices , 6000 Servers, etc.) and 10,000 non-IT devices. The hardware (servers/ databases/ respective storage and computing) planned to be supplied with the EMS solution should be capable to handle the data from these many number of IT and Non IT devices (including their alarms, backups, configurations etc. for duration of contract without any upgrade) . The solution should allow 50 simultaneous (concurrent) users while performing the CPU & RAM intensive operations and a capability to support futuristic scalability requirements.		
7	The OEM/OEM(s) should have their own IP rights on the solution being supplied, so as any customization required in solution may be possible by them . This will include integration with third-party Non-EMS / EMS applications over REST APIs /any other interface . The integration should be bi-directional in nature.		
8	The solution should be bundled with security measures to prevent any malware attacks, virus attacks, browser based attacks, ransomware attacks and data leaks in the provided solution. There should not be a need for installation of 3rd party software to comply and compensate the features.		
9	Should have the Asset management module which should be able to manage the all IT devices and Non IT devices . This asset management solution should be a comprehensive solution that allows to manage all devices as assets .		
10	Should be able to provide the change request (CR) management module.		

11	<p>The solution should be accessible via the intranet and internet in the secured manner. However, the solution i.e. any of the modules should not connect to Internet for accomplishing any required features asked in this solution e.g. fetching geo-maps for any functionality, and not even for the updates / upgrades etc. It should have in-built or capability to use custom maps as background and the updates/upgrades of the solution should be possible via non-internet mechanisms.</p> <p>Solution be bundled with Data base and Datastore encryption for Documents encryption and decryption using AES 256 bit cipher.</p> <p>The solution should only be accessed by secure browser supporting SSL 128 bit and SSL 256 bit encryption ciphers and without SSL there should be restriction/ control on the solution so as to prevent malware attacks, virus attacks, browser based attacks, ransomware attacks. The encryption should be performed via an industry standard ciphering algorithm. The solution must have in-built AES 256bit encryption for monitoring data and session within the platform.</p>		
12	<p>Deployment Mode of the Solution : The Module / Application provided should be capable to be deployed on physical server and/ or a virtual server.</p>		
13	<p>Bidder must ensure that all the hardware of different OEMs proposed in this bid and other bids referred in this bid's scope of work must be managed, monitored by the proposed DCIM & EMS solutions . The proposed solution(s) should be able to show the alarms from all system components envisaged to be supplied in this bid, including Phase-I and other bids referred in this tender. In general, solution should be OEM agnostic & should by default support integration with major OEMs of Network and server equipment and natively support SNMPv3 for other devices.</p>		
14	<p>Enterprise Management Solution (EMS) Specs</p>		
15	<p>Solution at devices (including servers) should be deployed in agent less mode . However, it should have agent based deployment support as well for any futuristic use case handling. The agent-less communication should be secured , wherever applicable it must be use SNMPv3.</p>		
16	<p>Should integrate with a proposed Automated Infrastructure management(AIM) solution (Comprising of Intelligent Cabling Management and other features) using REST APIs / SNMP so as the alarms,events can be monitored & managed from EMS. Bidder must also integrate with an already existing (Phase-1) AIM solution at DC (refer Scope of work for details). Integration should be on API level/SNMP without any requirement of installing any 3rd party software.</p>		

17	Should provide Network performance monitoring and diagnostics (NPMD) via reports and dashboards. It should support the reporting , status , threshold breach reports for all monitoring parameters for servers, Network elements. It should have features for proactive monitoring of network performance .		
18	The proposed solutions/Modules for the sought requirements should be able to run on latest versions of Microsoft windows or linux operating systems. All the updates and upgrades of the proposed solutions/Modules must also be supported on the upgraded / updated versions of OS during the entire contract period. The bidder also needs to provide the relevant software to ensure security of the provided hardware, software/ system. In case of any updates/upgrades of base OS, the supplied solution(s) must be updated/upgraded free of cost during the entire contract period. Also any bug fixes within support period must be supported. SI must ensure to update the patches or provision the upgrades via the non internet modes i.e. by following local update/upgrade mechanisms using HDDs/USBs .		
19	Should allow & perform integration with other third-party applications (such as AIM , DCIM etc.) through APIs. It must be ensured that all alarms arising out of any module of the solution should be sent to EMS and its database. e.g. If there is an alarm that arises in DCIM , it must be sent to EMS . The EMS must serve as an all alarm and event data base. Also, there should be a provision for Northbound and Southbound Integration Adaptors , gateways or CLI based integration for seamless integration and customization possibilities. System should have Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags additionally system should have options to do device grouping based on default fields and customer fields. No restriction in the number of level of grouping for the devices. provides the option to create the grouping based on the service offered to customer and map all the devices involved in the specific service till the component / resource level.		
20	The current performance state of the entire network & system infrastructure shall be visible in an integrated console of proposed solution		
21	It should provide a secured single login with unified console for seamless cross-functional navigation for all functions of components/modules offered across multiple areas of monitoring & management.		
22	Should be able to monitor network traffic by capturing flow data from network devices, such as but not limited to Cisco NetFlow v5 or v9, Juniper J-Flow, IPFIX, sFlow, sampled NetFlow data and Cisco ASA NetFlow.		

23	<p>Should support Network device or configuration management by supporting with Automated Backups of configurations, Change management in Real-Time , Allow execution of special Scripts (e.g execute sequence of commands in different devices for troubleshooting & creation of such scripts) , Compliance auditing & Automation of repetitive configuration management tasks</p> <p>The scripts should be allowed to run on single NE or can be issued in bulk on different set of NEs.</p> <p>The scripts may be used for upgrading the Firmware in NEs for any relevant issues such as fixing vulnerabilities.</p> <p>Additionally, the scripts functionality may be used for changing configurations, running and executing commands for troubleshooting or, so as it can automate configuration management , device management etc. by giving convenience to an operator / user for executing self created scripts.</p>		
24	Should also provide a feature of Remote Firmware upgrade on single or bulk devices		
25	Should monitor hardware and software health for Data Center Network & Server Equipment and should allow alarms, alerts and reports on hardware and software monitoring e.g. over system resource use beyond threshold limits, fault / alarm upon excessive network usage. May perform Hardware monitoring using Trap based integration with existing hardware monitoring solutions or element management solution supplied / asked from OEMs in this bid's scope of work.		
26	Should be an integrated solution for managing & monitoring devices , bandwidth utilization, configuration management.		
27	Should be able to perform Real-time monitoring of each of the alarms and resources (but not limited to such as CPU, Memory, Disk, IO, network etc. aspects) of physical and virtual servers including the other network devices		

28	The solution should have self-monitoring ability to track status of its critical components & parameters such as Up/Down status of its services, applications & servers, CPU utilization, Memory capacity, File system space, database Status, status monitoring between primary and secondary system and event processing etc. It should provide this information in real-time through graphical dashboards, events/alarms as well as in the form of historical reports. Reports shall contain visualizations utilizing the applicable graphic types such as Bar Chart, Gauge , Pie Chart, Scatter Plot, Simple Value, Table, Time Series, User Image, User Text etc.		
29	The proposed solution should be able to monitor Physical Servers running UNIX , Linux ,windows or any other operating systems & also Virtual Servers on VMware or any other Hypervisor-based Virtual Network Function infrastructure network management must also be supported .		
30	Supplied Solution should monitor the devices/VMs continuously and identify & capture the faults/alarms from each of it.		
31	There should not be any agent on the managed node , and the overall solution must provide the system performance data. For event management it should be able to prioritize events, perform duplicate suppression ability to buffer alarms .		
32	Users must be able to choose the thresholds (high and low) for when an alarm and/or warning will activate, along with the points for the severity level. Users must be able to acknowledge and filter alarms. Alarms should have a way to prioritize more important alarms. The solution shall include an alarm history page where all system alarms are stored. Users should be able to search for previous alarms by site, device, or point. should be able to manage and display alarms/events/alerts, store them and should allow creation of new alarms/events/alerts from scratch with customizable threshold limits. The threshold may be applied to any valid parameters which are being monitored per device .		

33	Should Support Assignment of Alarms/events/Alerts to System Administrators for processing and completion via a Helpdesk / Service Desk feature . It must also allow the logging/recording of solution/Actions during Alarm/event/Alert Completion/closure. As an hypothetical example, after the analysis of Alarm/event/Alert, if solution requires a change in configuration at a Network Element(NE) , this change in configuration should flow via the change management system for ensuring appropriate approvals and recording . A ticket for this alarm should be created in helpdesk, which should trigger a Change Request in Configuration Change Management system . Upon various approvals , the CR is implemented in the system and only then CR , ticket and alarm are closed . CMDB is updated with this configuration change for future records . User must also be able to map an Alarm/event/Alert with a ticket as well as CR.		
34	Should support to have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, sending SMS text alerts, playing sound, emailing any type of reports generated etc.		
35	Should Support Alert Escalation through defined Escalation Metrics		
36	Should Generate Green Alerts / automatic update the alert status as down / indicate the new status after successful alert processing		
37	Should support variables in alert email messages to make message self-explanatory		
38	Should be able to define relationships (based on topology, etc.) between servers and applications to avoid false-positive email alerts in case of outage		
39	Proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored. The solution must also allow for the customized reports in addition to default reports as per templates. System should be able to generate the current alarm reports for entire inventory or per device basis. Same for the historical data with custom time period.		
40	Should allow advanced customization by providing options to enter custom queries to extract data from database directly		
41	Should allow sending out (emailing) of all types of reports on custom schedule such as daily, weekly, monthly basis etc.		

42	Should allow Creation of Customized dashboards as per requirement		
43	Solution should provide feature that facilitates suppression/reduction of alarms displayed by means of alarm suppression feature . For example, during a maintenance , it should allow to suppress alarms from devices. The system must support filtering options by alarm status , device type/category to facilitate quick actions .		
44	The proposed system shall integrate network , servers or other equipment alarm/performance information in a single console/dashboard and provide a unified reporting interface for each category of components.		
45	Alarms should be mapped to the live topology views and real time updates to topology based on alarm occurrences. System can support one click alarm masking capability.		
46	Should trigger (pre-configured and customized) automated actions based on incoming events / traps. These actions can be automated scripts/batch files. Scripts/batch files should be customizable.		
47	Should support out of the box network Trap Analytics		
48	Tool should support automated Change Plans including but not limited to: Conditions to validate, Pre-Change Validation, Change Script (similar to legacy Command Script), Post-Change Validation, Rollback Script		
49	Should provide the comparison views for configuration versions e.g. Original Configuration Vs Latest Configuration		
50	Should provide Compliance Model w.r.t Configuration, Software, Running State		
51	Should provide Risk Visibility Dashboards of network infrastructure		
52	EMS solution proposed should have capability to fetch / receive alarms from other Network Monitoring tools / Systems monitoring tools / other domain monitoring tools like AIM , DCIM solutions supplied as a part of this bid and including equipment from other locations / bid as defined earlier in this document and /or as per scope of work.		
53	Alarm Filtering should allow flexible filtering rules for users to filter the alarms by category, severity, elements, duration, by user, by views, by location or by any other custom field of choice present in the alarm object		

54	The discovery processes may be configurable to perform continuous and auto discoveries. Should be able to auto discover, monitor devices installed and commissioned at different Physical locations		
55	Should have an Asset management system for maintaining and managing the all assets as defined in the scope of work .		
56	The EMS solution should be integrated with DCIM solution detect physical assets movement from racks and receiving alarms from DCIM / RLPAT Solution .		
57	Should be able to integrate with modules serving other monitoring/ management purposes and consolidate the information into a single view such as should be able to integrate with the AIM solution over REST APIs/other mechanisms to receive alarms from AIM.		
58	Should be scalable to allow the addition/integration of new instances of devices to be added in future		
59	Should allow information from multiple instances of application to be consolidated into a single view		
60	The EMS solution should integrate with Network Equipment's OEM supplied Element Management systems. Bidder needs to provide the Network Equipment's OEM supplied Element Management systems along with the NEs. Also, SI may budget to integrate the proposed EMS in this bid with other Element Management Systems / Network Management Systems solutions supplied earlier w.r.t other Phase-1 bids / Infra referred in this bid.		
61	It should monitor performance across heterogeneous networks		
62	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, Servers etc.) and map the connectivity between them with granular visibility up to individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices. It must support auto Discovery of network inventory and create a network topology		
63	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.		

64	<p>EMS should provide the compliance management report in the integrated view showing network topologies . The Network configuration manager should allow the overall network to stay compliant with current day industry standards like HIPAA, SOX, PCI etc. by using compliance templates that allow to fix vulnerabilities in the network , Prevent any loop holes in a Configurations or any other issues.</p> <p>The SI is required to provide a clean VAPT report of the complete solution(i.e. including all modules) at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done , upon any major upgrade in solution or solution’s respective modules.</p>		
65	<p>EMS's Network Configuration Analysis feature should allow Network Configuration Analysis Reports that help to diagnose and resolve faulty configurations such as reports on all network devices that have a startup-running conflict (don't have a sync) as well as the ones that have their startup and running configurations in sync. It should also be able to provide reports on Configuration Change Trend –a report that provides the historical trend of all configuration changes during a specific time period , aiming to allow to manage network better by performing extensive / in-depth configuration analysis on all device types in network.</p>		
66	<p>The system must be able to build and visualize network topology using SNMP, information in ARP tables from routers, MAC tables from layer 2 switches. The discovery should be automated and continuous.</p>		
67	<p>It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across MPLS and or any further Network connectivity’s planned in future.</p>		
68	<p>The tool should support dual-stack (IPv4&IPv6) shall be able to discover IPv4 only, IPv6 only as well as devices in dual-stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.</p>		

69	The tool shall also be able to work on SNMP v1, v2c & v3 based on the SNMP versions so as proposed solution is able to monitor and manage the supplied equipment/devices as per the RFP. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP. It should also support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery.		
70	Solution must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms		
71	The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices.		
72	Should be able to create and allow management of Service requests by integrating with the IT Helpdesk solution/module. Must have Email-to-Incident feature, allowing automatic conversion of emails to tickets. Must maintain a single thread not only on per ticket Id basis. but also on email sender, cc responses to that email chain.		
73	Must have the following Device (especially for Networking Devices) Monitoring Capabilities . Should be able to generate alarms based if any of the parameters being monitored goes out of threshold range. These parameters should be allowed to record in a report for a selected time duration. The reports should be allowed for performance issues observed while monitoring during a specified period of time (performance reports). The performance reports should also be allowed for only a specified group of devices.		
74	i. Device Monitoring parameters such as a Device status and Availability , b CPU Load Data , c Device Disk Space Data ,d Memory Utilization etc.		
75	ii. Device Hardware Monitoring such as a Device Fan Monitoring , b Device Temperature Monitoring ,c Power Supply Monitoring etc.		
76	Link Monitoring : Graphically represent the various links over geographical maps. Each link's information on status and latest alarms generated shall be presented to give a quick bird's eye view of entire link health. These parameters should be allowed to record in a report as well. Should be able to generate alarms based if any of the parameters being monitored goes out of threshold range.		

77	Solution should allow per link parameters such as a Link Availability Monitoring b Average Response Time Data for each link c Bandwidth Utilization Monitoring d Network Latency Data e Network Topology f Packet Loss Data g Network Discard Data, Error Rate etc.		
78	Should allow to generate Link Monitoring Reports with parameters such as a Performance Data Analysis ,b Performance Data Collection , c Performance Report Generation ,d Traffic Analysis e Utilization and Error Rates .		
79	Should support Bandwidth Monitoring with parameters such as : a Network flow analysis ,b Netflow collector , c Sflow collector d Jflow collector e Real time monitoring f Bandwidth Utilization etc.		
80	Should support bandwidth Monitoring Reports with parameters : a API for data extraction , b Single click instant reports ,c Usage history based on hours minutes days , d Top talkers report , e Top Listeners report , f Top users report , g Top hosts report , h Protocol/Application level reports , i Interface level reports , j Customised reports , k Customised email alerts, l Application Mapping, m Device Grouping etc.		
81	Solutions should allow to maintain Logs such as : a Historical Logs in respective modules, b Interface Error Data/ logs ,c Syslog Messages Solution should have an inbuilt feature of an integrated SysLogServer, i.e. EMS solution should be configured to receive individual syslogs from different systems/solutions/devices. It should be able to parse the SysLogs based on the parameters defined/configured and is able to show the alerts/critical/alarms etc. as per configuration in EMS. In case of no inbuilt feature of a SysLog Server, the OEM may integrate an enterprise grade Syslog server, test and create a customized solution for above requirement.		
82	It should be able to capture, track & analyze traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc. required as a part of Network Traffic Flow analysis system.		
83	It shall provide key performance monitoring capabilities by giving detailed insight into the application traffic flowing over the network.		

84	Should monitor Virtual Private Networks (L3, L2), VLANs, MPLS service availability and inventory. It should support in end to end management and view of IPSec tunnels . It should support monitoring of connectivity of all the network elements / servers / other IP equipment as per scope of work		
85	Should provide inventory view of L3 VPNs, detailed views per L3 VPN. Should be allowed to be exported to reports		
86	EMS solution must have the capability to import MIBs of 3rd party Data Center components so as trap monitoring can be enabled.		
87	Access Privileges and Roles for different users/operators		
88	Each user/ operator should be allowed to provide with user roles that should include operational service views enabling operators to quickly determine impact and root cause associated with events.		
89	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS besides GUI/browser.		
90	Permissions and Features to access the system should be defined within the roles / based on roles and access privileges definer per user basis.		
91	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.		
92	Solution should visualize server, network, storage, and logical application environments and dependencies and compliance state.		
93	Besides the alarms per device the solution should be able to provide per device virtual visualization of interfaces, management interfaces, interface status, link status etc.		
94	In addition, the solution should be able to provide the power status of each device. In case of multiple power modules per device, multiple power status per device should be shown.		
95	Provides Layer 2 and virtual LAN (VLAN) network information. Should be allowed to be exported to reports		
96	Should provide out of the box Reporting such as: <ul style="list-style-type: none"> • Site-to-site quality-of-service reports using any inbuilt tools within supplied modules. • VPN / IPSec reports 		
97	EMS module shall allow all types of reports to be exported to .pdf & comma-separated values (.CSV) formats.		

98	Reports generation should be customizable , so as to allow to choose the fields/columns/parameters per report.		
99	Should provide agentless discovery and shall use Industry-standard protocols such as WMI, SNMP, JMX, SSH etc. to perform discovery		
100	The solution must have the ability to add network devices into inventory via auto discovery or the auto discovered devices into the inventory (if not yet added to inventory)		
101	Network Traffic Flow Analysis System		
102	It shall be able to capture, track & analyse traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.		
103	It shall provide key performance monitoring capabilities by giving detailed insight into the application traffic flowing over the network.		
104	It shall be able to monitor each interface status per device, network fault at device level, per device basis - network traffic utilization , packet size distribution, protocol distribution, application distribution, top talkers etc. for network traffic. It should be able to generate reports for above stats.		
105	It shall collect the real-time network flow data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.		
106	The platform must provide complete cross-domain visibility of IT infrastructure issues		
107	The platform must consolidate monitoring events from across layers such as Network, Server, Database, 3rd party tools (monitoring solutions to monitor key DC elements like wires etc.)		
108	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases		
109	The solution must support custom dashboards for different role users such as Management, admin and report users		
110	The solution must allow creating custom data widgets to visualize data with custom preferences		
111	The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.		
112	The solution should provide top level view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console		

113	The reporting and dashboard module of the solution must have capability to integrate with 3rd party data center monitoring solutions. Bidder needs to integrate EMS with proposed DCIM solution, Element Management solutions provided by OEM's w.r.t NEs proposed in this bid & NEs of phase-1 bid (if element management system is available via phase-1 bid) & also incorporate the MIBs of NEs proposed in this bid.		
114	Upon the integration with DCIM solution, the EMS solution should have the capability to present critical metrics w.r.t Data Center infrastructure in the form of a dashboard to gain visibility into overall health of the other infra components.		
115	The solution must support visually representing network outages and other error conditions on the topological map. In General , Solution should be able to generate alarms based on if any of the parameters being monitored goes out of configured threshold / threshold range.		
116	Provision the following Device Performance Monitoring Capabilities for Servers (Application/Historical /others) & Integration with OEM's Element Management solutions to achieve described monitors from installed servers , is also the scope of requirements.		
117	1 Physical Server Monitoring parameters such as a. Server Status and Availability , b. CPU Utilization c.Memory Utilization d. Process Monitoring e. File System Monitoring f. Disk Utilization etc.		
118	2 VMware and ESXi Host Monitoring parameters such as a. Status and Availability b.CPU Utilization c. Memory Utilization d. Monitoring of Virtual Hosts e.Disk Utilization f.Network Utilization g. Hardware Monitoring h.Performance Dashboard i.VM Replication Monitoring etc.		
119	3 Linux server Monitoring parameters such as a. Server Status and Availability , b. CPU Utilization , c. Memory Utilization ,d. Process Monitoring ,e. File System Monitoring ,f. Disk Utilization ,g. Network Interface Monitoring etc.		
120	4 Windows server Monitoring such as a Server Status and Availability b CPU Utilization c Memory Utilization d Process Monitoring e File System Monitoring f Disk Utilization g Network Interface Monitoring h Event Log Monitoring etc.		
121	5 Database Monitoring parameters such as a Database Availability b Database Process and Logs c Locks and Buffers d Tablespace/Database e Sessions/Connections f Database Memory h SQL Statistics i Database Jobs etc.		

122	6 SSL Certificate Monitoring or SSL Certificate Inventory Management for its attributes such as a. expiry b. Availability c. Validity d. Certificate Information		
123	7. SLA Management parameters such as a Customized SLA for Applications , b SLA escalation ,c SLA Reporting feature to provide downtime per equipment , link etc. primarily for cases, where tickets due to alarms are sent to ticketing tool etc.		
124	EOL and EOS Management - Keep track of all devices (networking, servers and other equipment) for their end of Life , end of Sale, and end of Support.		
125	Should be able to integrate with Service Desk module to support and handle large volume of incident, event, service requests, changes, etc.		
126	Network Configuration Module		
127	Should allow Network Configuration change management on multiple vendor devices for all the hardware equipment as stated in the 'General Requirements' of this document. Change management should include the tracking and version maintenance of configuration changes in real-time on each of them.		
128	It should allow to audit configurations and deploy configuration updates in single or multiple devices at once. From the scalability perspective, purposed solution should support managing configurations of hardware of more than 200 different OEMs , including all major OEMs .		
129	It should have enhanced network security by preventing unauthorized configuration changes and notifying the admin about any changes .		
130	The proposed management solution's network configuration module, which should be able to automatically backup configurations (for both text based and binary configuration files etc.) on routers, switches, firewall, access points and other network devices. The trigger to automatic back up may be setup in EMS such trigger could be upon a detection of a configuration change and/or an automatic timer based. The configuration change should be recorded with the date-time stamp along with the user info.		
131	Should be able to backup, compare and restore network configuration for all the networking devices defined as per scope of work of this tender. Backup system should allow to store for atleast 1 year of historical data. Further, it should be a provision on the tool for configuring the data retention and log archival so that operator(s) may be able to control as per its discretion.		

132	Should be able to make single or bulk configuration changes across multiple devices. For example: such as change community strings, update ACLs etc. Also, in case a user changes the configuration on a NE, the EMS's Configuration change management module should be able to detect this change per user basis. It should be able to display the new configuration , show its difference with old configuration version and also show which user made the changes at what time etc.		
133	The system should be able to clearly identify configuration changes / policy violations / inventory changes across the network of networking devices from multiple OEMs .		
134	The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “start-up” configurations and alert the administrators.		
135	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the administrative tasks (such as mentioned below) of effecting configuration changes to network elements: a) Capture running configuration b) Capture start-up configuration c) Upload configuration d) Write start-up configuration e) Upload firmware		
136	The proposed solution must able to merge configuration changes & load it to multiple network devices		
137	Should allow automated and scheduled backups of configuration files , it should tend to eliminate manual configuration management , by allowing features such as and not limited to - scripts , automation etc.		
138	Should allow to Encrypt and store configuration files in enterprise standard and internationally complaint standards. The users session and data on the storage should also be encrypted including the support terminal session or shell session .		
139	Should allow to setup / mark a configuration as the best working "Baseline Configuration" , so as to allow for a quick backup during a disaster / crisis event.		

140	Should provide configuration mechanisms that allow roll back to a selected 'marked' working configuration version or any baseline configuration whenever any configuration change is unsatisfactory.		
141	Should follow configuration versioning and comparison between saved versions		
142	Should support Network Configuration Analysis: Should allow through in-depth analysis of configurations.		
143	In the integrated Configuration Analysis module it should allow to perform configuration analysis for network equipment's like router's and switches. The configuration management module should also be integrated with AAA/AD server for providing RBAC. The solution should be completely multi-tenant in every module for allowing RBAC. There should be logging of each command performed at any NE by the users . This should be logged and reported at AAA server.		
144	The system should be able to capture the configurations in the database/datastore.		
145	The system should be able to differentiate the old and current configuration with version control.		
146	The system should be able to capture exact configuration change with color coded highlights, and date and time of addition, modifications, removal or change in the configuration.		
147	The system should be able to provide the reports for various actions described under Network configuration management feature. The reports may include status and summaries of different activities such as device configuration details, changes in configuration (within a specified period / per user basis), network inventory, conflict between startup and running configuration, device audit details, policy compliance details etc.		
148	The system should be able to export the configurations in TXT , CSV , PDF formats.		
149	Description for IPAM & Switch Port Management Specs		
150	The IPAM Solution must support 65,000 IP Address Management for both IPv4 & IPv6 together. It should be scalable upto 1,80,000 without any hardware change.		
151	The solution must be agentless can be an pre-integrated module of EMS or it could be a separate module .		
152	The IPAM solution must be run on high availability as per previously suggested architecture for HA in this document.		

153	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.		
154	The solution must include an application programming interface (API) in order to interface with IT Helpdesk / network and/or asset management systems, a configuration/change management database (CMDB) solution or other applications. In General, the overall system should support REST APIs(PUSH and PULL) for integration with 3rd party systems such as EMS or otherwise the proposed IPAM module may be a part of EMS system itself.		
155	The IPAM solution should be able to seamlessly integrate with DNS and DHCP records.		
156	It should support the features such as : Creating groups, Subnet ,Adding subnet to group , Automatically detect devices ,Manual/Automatic assigning the IP to the device interface , Manually adding the device, Display Interface name with IP address , Scanning devices in the network , IP address scanning within the subnet or IP address scanning within the group etc.		
157	The IPAM solution should be able to create its own widget / report to display customized subnet reports that should include details such as free IP, used IP and per IP Address details such as DNS name, Last alive time, Status(Used, Unused) etc. i.e any other custom fields added		
158	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. IPAM system should support VLSM (Variable Length Subnet Masks)		
159	IPAM user interface must be web-based without specific browser vendor requirements		
160	In General , the history and backup data w.r.t IP Address Management Tool and Switch Port Management Tool should be saved for atleast 1 year and The IPAM shall have inbuilt adequate security tools to avoid any unauthorized access to the system in particular and solution as a whole .		
161	IPAM system should be able to export reports in PDF, CSV format and in any other formats		
162	IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability. It must allow to create different user profiles with different level of permissions. Preferably, it should integrate with AAA/AD to achieve this feature.		
163	The system's audit records should contain a timestamp, username and record modified.		
164	The system's reporting engine should include audit reports.		

165	The system should support granular rights administration, limiting the functions and rights to user and/or Zone level by integrating with Active Directory.		
166	The tool should show up and map the devices plugged into each switch port in real-time		
167	Should allow admins to find out which devices were connected to a particular switch at a specified period of time		
168	Advanced search mechanisms should allow the devices searching by MAC, IP Address, DNS Name etc.		
169	Allow grouping of switches for easy identification and control		
170	The IPAM tool should be able to perform and track address space allocations in accordance with routing topology to model and optimize route aggregation.		
171	Should provide notifications upon Switch port status changes		
172	Should allow to Manage Switch Port using SNMP by allowing administrators to block or unblock a switch port		
173	The IPAM component must perform host discovery using a variety of methods including ping, TCP port 80 connections, Address Resolution Protocol (ARP), cache data, and device OS mapping etc.		
174	MAC Address Scan - The tool must have the ability to scan a given range of IP Addresses and display the MAC addresses for various devices available in the given range. Also must display the IP address, port number, community, MAC address, DNS name, system name, and system type.		
175	DHCP Scope Monitor - The tool must be fully integrated with the DHCP system and support the capability to fetch all the scopes that are defined in the DHCP Server and display the total, used, and available IP Addresses in each scope. When the number of available IP addresses falls below a defined value, the display should indicate the criticality.		
176	The IPAM must have the capability to find free address space across a range.		
177	The IPAM must scan multiple subnets simultaneously . It should be able to make out which IP address have been assigned statically .		
178	It must provide the requisite information to EMS to build and visualize network topology using information in ARP tables from routers, MAC tables from layer 2 switches.		
179	The system must have the capability to group the subnets in a hierarchical tree format		

180	It should be able to handle Device/Network templates (Creation, Deletion, Modification & Uploading) and the system must automatically discover the network's subnets or import them from a CSV file		
181	DNS Resolver – The IPAM tool must provide the host name of any node whose IP Address is known and vice versa with additional details like the default net mask, network type, and the status for the forward and reverse lookups		
182	DNS Scan – Using this tool one must be able to scan a range of IP addresses to see whether the forward and reverse lookup actions are working fine for the devices. It should show the response time. In cases where an IP is not used in the network, the tool must prompt that the system does not exist in the network.		
183	The IPAM shall support appropriate logging functionality on itself as well as on external source like Syslog servers. All the activities made by administrators must be logged inside an Admin Audit Log Report.		
184	The IPAM must provide integration with Vmware, HyperV, Openstack etc. and discover the VMs with clientless integration . The solution must provide details of virtual servers / VMware server running Linux or Windows as deployment of a virtual appliance		
185	Asset Inventory Monitoring & Management		
186	An asset management module should be in-built part of proposed EMS from same EMS OEM.		
187	System shall have an ability to track (automatic/manual/via integration with other modules of overall system) and manage all data center and remote location assets including but not limited to IT/IoT/Non IT/Software(s) - Racks, Network equipment, IT equipment, Intelligent PDUs, sensors, application(s) etc.		
188	System should allow to search / locate a data center asset based on various filters/fields, it should also provide detailed information about the assets. It should allow a provision / feature with ability to define down time for Assets to conduct Maintenance activities.		
189	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.		

190	Should provide the compliance management report in the integrated view showing network topologies.		
191	The tool shall be able to work on SNMP v1, v2c & v3 based on the SNMP version supported by the device. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP. It should also support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP/ Trap based discovery. Solution should be able to integrate with EMS to auto discover the IT Assets via its scan/discovery process		
192	Solution should allow to manage the physical aspects of all IT assets & Non IT Assets —from request of movement , to their end of Life , Sale, & Support related timely triggers, making it easier to optimize costs, mitigate security, and compliance risks.		
193	Assets and Non IT Assets will include category of devices as defined in scope of work such as Network switches, routers, firewalls, application servers, historical servers, packet brokers, etc.		
194	The Asset system should allow Role based access.		
195	While performing discovery, solution must also allow for a feature that allows to include and exclude IP addresses / subnets or devices from auto discovery.		
196	The proposed solution must provide a detailed asset report with different filters mechanisms, organized by vendor name, device type, listing all ports for all devices. Should be able to create Service requests for each of the asset.		
197	Tool should provide the information about equipment's dependency on each other. This affects the overall performance of the datacenter. Performance data of each equipment in the datacenter should be available for analysis. Thus any product vendor for an underperforming asset can be alerted and the inventory is either repaired to perform or replaced in time . Alerts for such scenarios should be generated in EMS system		
198	It must easily and automatically discover newly add devices to the n/w.		
199	The system shall provide an easy method of searching and locating assets and asset groups		
200	The system shall support an importing of asset list from a 3rd party tool in CSV format into an asset database. If a specific asset in not defined, the tool shall be able to create it.		

201	The system should allow the user to create Asset profile with unique serial no, asset tag, asset owner, asset life, details of assets etc. The assets must be searchable with any of the parameters such as serial number , asset tag . It must allow to list out assets based on owners , location etc.		
202	The system should allow the user to search & track assets at any time to know the status of an asset – location, assigned to which user, contracts/warranty/AMC renewal for maintenance etc.		
203	Overall system's solution should support virtual installation or server based installation. This should not be a proprietary hardware based or embedded based solution.		
204	Change Management (CM) Module Requirements		
205	The CM solution could be a module within EMS supplied. The CM solution should be web based , must also work in HA mode.		
206	Solution should allow to create different roles (preferably after integrating with AAA/AD) with different privileges such as Change Requester , Change Record Authorizer, Change Implementer , Change Advisory Board Member , Change Manager , Post Implementation Reviewer , Customer Approver , Customer Tester , WorkFlow Administrator etc. This will ensure the restricted access to devices. Different privileged users should be able to play the role of implementers, reviewers, approver etc. , so as to allow a workflow w.r.t change request. Change management must be implemented in conjunction with configuration management, so as wherever required, a view of the infrastructure may be provided to assess an impact of a change.		
207	CM should allow to Create, View , Edit the Change Requests (CRs) .		
208	Each CR must be allowed to follow a chosen / predefined workflow . The solution may also allow to create work flow for CR.		
209	The solution must facilitate Assigning of roles to ensure that a change process workflow is started, managed, and implemented by the right people .		
210	The solution must provide Change history: Captures the change history of all the fields and can be viewed for each record. Audit trails like changes done by the user, modification time, current value and previous values.		
211	The solution should have CR correlation: Linking of CRs to related incidents, problems, assets, Cis		

212	CRs must support Multi Stage custom based approvals.		
213	The solution should Achieve complete visibility into which CIs have changed.		
214	The solution must have defined Standard Reports		
215	CRs should be authorized by Authorizer before taken up further in CM system		
216	Change Advisory Board Member is able to sign-off, reject, or recommend changes necessary for anything that need to be processed.		
217	Should be able to provide the status of all CRs (Open, Close, etc.) in a view . It should be filterable per user basis .		
218	The system shall have integrated ITIL v3 or higher processes complied Operations Management System for Helpdesk, Ticketing, Maintenance and Configuration Management Database (CMDB). The system shall enforce best practices workflow and meet ITIL framework guidelines. All monitoring elements should be stored and accessed from a central datastore. This also should be have RBAC.		
219	Change Implementer Implements the change and updates the status. In General, the status change of a CR triggers the email request to its configured workflow owners and assigns the new 'action owner'		
220	Change manager is able to review all the CRs, sets Change Record Authorizers, forwards the CRs to the CAB, issues Change Schedules related with CRs , reviews all the implemented CRs, and Generates Regular Reports		
221	Customer Approver(s) is able to review and approve the CR before the CR is implemented.		
222	Customer Tester is able to update the result for a CR		
223	The solution must Assign downtime time start and end for a CI(Configuration Item)		
224	The solution should be able to allow Assign Priority, impact, urgency and risk to CRs		
225	Solution should have its own application and data base . It should be a web based portal hosted in an on premise manner.		
226	CM Module should allow the end users to create, update, search and get status update of change requests. It should allow the attachments of documentation (such as pdfs etc.) with the CM requests		

227	It should be able to use IMAP, POP3 ,SMTP protocols to provide email integration and able to send emails for CRs status as configured . The solution must be able to use IMAP, POP, protocols & should be able to automatically convert service request emails into help desk tickets.		
228	CMS should be integrated with overall solution or be in-built as a part of EMS.		
229	Supplied solution should have a standard search , advance search mechanism on the fields for enhanced productivity.		
230	Should be able to well integrate with the supplied IT Helpdesk / Service Management solution to achieve the overall functionality. This is to ensure that a mapping between Ticket & CR can be made. On same lines, in case the CR is created in the Change Management Solution it should trigger an automatic Ticket creation in IT Helpdesk solution.		
231	Supplied solution should be able to generate insightful reports on changes, compliance, inventory and other vital network parameters.		
232	Supplied solution should allow atleast backup / history database maintained for atleast 1 year including but not limited to configurations, alarms, services , assets, asset locations, network performance related database		
233	The EMS system as a whole should be able to send notifications on GUI, email and SMS		
234	The supplied CM solution should be provided with a hardware capability to support 15000 service requests in a day with at least 50 simultaneous users . Hardware supplied should be capable enough to store data at least for 1 year.		
235	Features for IT Service Management (ITSM) / IT helpdesk solution for managing the day to day Operations		
236	The solution should have its own IT Service Management (ITSM) / IT helpdesk solution which is based on ITIL best practices.Should provide an GUI interface w.r.t emails. The ITSM system shall be capable of assigning, tracking tickets to users manually as well as automatically based on predefined rules, and shall support notification and escalation over email. E.g. A ticket with 'Network fault' as a keyword(s) tickets gets automatically assigned to a user whose role is configured network technician.		
237	IT Service Management solution must be an industry standard, enterprise grade web based solution that enables end users to create service requests and must be placed in High Availability Mode as sought in General requirements.		

238	<p>The ITSM solution proposed should be designed & architected so as to allow to use ITIL framework and processes across sought modules including DCIM / EMS , Alarm / Incident Management, Asset Management , CMDB etc. , so as unique data and workflows can be maintained for overall solution.</p> <p>The ITSM solution should automatically provide suggested knowledge base articles based on Incident properties/attributes/tags/keywords etc.</p> <p>The ITSM solution must integrate with all the supplied and required modules such as DCIM,EMS,AIM,IPAM,CMS,RLPAT solutions etc .</p>		
239	<p>There should be a database in place to store data w.r.t integrated Tickets, Alarms , Incident & Problem management, Service Level management/ targets , configuration data base etc. The ITSM tool should allow to export the ticket reports in different formats such as HTML,PDF ,Excel etc.</p>		
240	<p>The ITSM solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.</p>		
241	<p>The system should be able to create service desk tickets/ work orders/approval receipts for any work to be done in data center. For example - mounting a new server, connecting it to specific ports on network, powering it ON from specific outlets of the iPDU etc. This workflow should have various pre-defined approvers/reviewers / implementers etc , who should be able to approve/ disapprove/ comment(add remarks etc.) . The tickets templates should be customizable .The system should allow to edit , assign , search and track these tickets. It should allow to provide dash boards with different filtering options that also allow to take out customized reports such as w.r.t ticket status , groups / user wise assignments etc.</p> <p>System should also allow to search a ticket and track its historical details of various actions performed on same.</p>		
242	<p>The ITSM solution should provide to browse through Configuration Management Database (CMDB) which should offer powerful search capabilities for configuration items (CIs) and services, enabling to quickly find Configuration Item as well as their relationships to other CIs.</p>		
243	<p>Configuration item should get automatically attached with the ticket to enable the support team for faster resolution.</p>		

244	ITSM solution should provide an option for adding new workflows/catalogues with custom SLAs & multistage approvals. The workflows / catalogues may be based on hierarchy, roles , category of service request per catalogue. It should include notification and escalation capability if approval is not performed within the defined time period. Tool should be able to send alerts via SNMP Trap. Must support XML notifications, Pop-up window and Audio alert.		
245	The ITSM Solution should be a web based solution and should be accessible via the browser.		
246	ITSM solution should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, CI, location, or customer. Solution should be able to provide the aging reports of the tickets based on various types/categories of tickets. The Notification mechanism should allow administrator to define notification channel per time of day and trigger multiple notifications per person.		
247	Solution should provide modern data analysis methods for insights and adding value to service desk .		
248	The solution should be able to record the actions of users per session basis including details such as time stamp etc. as per user for audits and records purposes.		
249	Integrates with any underlying service management solution including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.		
	General Features II		
250	The EMS solution should be able to group devices into different categories.		
251	The EMS solution must display the topological information in graphical form representing nodes and groups of nodes on a realistic geographical map.		
252	Uses the communications channel with enhanced security features, audit logs, and access control policies to provide direct connections to servers in any location.		
253	The system (IT Helpdesk system, etc.) shall allow to create request and work orders (and approvals) with customizable task details and timelines so as to allow measurement of the time taken for a task/work completion or equipment / service downtime and hereby allowing the calculation of SLA and penalties via the tool. The IT Helpdesk system should allow the attachments of documentation (such as pdfs etc.) with the CM requests .		
254	The IT Helpdesk system should also be integrated with AD/LDAP for providing the access to users		
255	The system should support filtering options to search and list down tickets.		

256	<p>The system should have a SLA Management module. The system should provide the operator ease of access on SLA creation for nodes and services. Escalation should be configurable and optimized for day-to-day operations. It should allow to add formulas for helping any calculation in SLA / downtime . SLA module should be customizable to provide the penalty details as per SLA criteria mentioned in the tender. The provided reports are ready to be used for penalty calculations.</p>		
257	<p>Collaboration and Knowledge-based module - The system should also have knowledge-based module built in for the operators for quick issue identifications and resolution, thus minimizing the time and efforts. This will should server as a historical database and used for training of new recruits, resolution of alarms, resolution of certain specific issues. Users should be able to add information, categorize it, add files to it. The proposed storage for Collaboration and Knowledge-based module artifacts should be scalable. It must sufficient enough by default to store data for the complete contract period. In case of any shortage of storage , SI will be required to immediately(within 1week notice) provide the double the original capacity storage base.</p>		
258	<p>The applications (solution) per hardware should be installed as follows and must work in High Availability Mode: The bidder may also suggest the optimized solution for effective/smooth execution of modules/application. However , it will be decision of ERNET India will be final in this regard. Server#One to host apps : DCIM+RLPAT Solution+ Solution for Heat and Humidity Sensors.</p> <p>Server#Two to host apps : EMS(including its all components such as Network Device Management, Device Configuration Management, Network Performance Management , IPAM, Switch Port Management, Change Management, Network Asset Management etc.) , Automated Infrastructure Management etc. The AIM is also allowed to be installed on a separate server as well.</p> <p>Server#Three to host apps : IT Helpdesk Tool.</p> <p>Server#Four to host apps : AAA Server.</p> <p>Server#Five to host apps : Active Directory (with DNS , DHCP etc.) - may be combined in Server # Four in a VM based configuration.</p> <p>A replica of above is to be provided at DR.</p>		

	OEMs having all required modules of EMS in a single software , is allowed to provide all EMS modules on a single server .		
259.	OEM of EMS Solution should be ISO 27001,ISO 27034 certified.		
260.	OEM should be atleast CMMI Level 3		

PART -C Manpower Specification

Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi

Sl.No	Role	Min. Qualification, Relevant Experience & Certifications	Compliance (Yes/No)
1	Project Manager	B.E./B.Tech/MCA 8 Years relevant experience in IT/ITeS (minimum 6 years' experience for managing large data centers) + CCNP-DC/ JNCIA-DC or equivalent Certified	
2	Security Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience in IT Network Management + Certification: OEM certified engineer on proposed security equipment Such as JNCIP- SEC, Fortigate NSE 4, CCNP Security or equivalent	
3	Network Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience in IT Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 5 years of work experience on leaf and spine architecture	

4	Network Engineer	B.E./B.Tech/MCA in Computer/IT / Electronics + 4 Years relevant experience in Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 3 years of work experience on leaf and spine architecture	
5	System (Server) Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience of different flavors of OS with Storage + Must have 5 year of experience on offered OEM Servers.	
6	System (Server) Engineer	B.E./B.Tech/MCA in Computer/IT / Electronics + 5 Years relevant experience of different flavors of OS with Storage + Must have 3 year of experience on offered OEM Servers.	
7	EMS & DCIM Engineer	B.E./B.Tech/MCA + 3 Years relevant experience + Proposed EMS certified engineer, if any or Should have CCNA/JNCIA or equivalent certification.	
8	Help Desk Support Staff	B.E./B.Tech/ MCA in Computer/IT / Electronics with 3 Year relevant experience.	

Section VI: Qualification Criteria

A. Bidder's Qualification Criteria

1. The Bidder must have valid ISO 9001:2015, ISO 20000, ISO 27001:2013 Certificates. *Bidder shall submit the valid documents.*
2. Copy of Board Resolution and/ or registered Power of Attorney for authorized signatory which authorizes the signatory to commit and submit bids on behalf of the bidder shall be submitted along with technical bid; ***failing which, the bid will be liable to be rejected.***
3. The minimum average annual audited financial turnover from of the bidder during the last three years (FY 19-20, 20-21,21-22), should not be less than Rs. 500 Crore. The bidder should also have Positive Net Worth of Rs. 50 Crore as on 31/03/2022. A certificate from a practicing Chartered Accountant (with UDIN) on its letter *head confirming annual turnover, average turnover for 3 years as specified above and net worth as on 31/03/2022 is to be provided along with the technical bid.*
4. Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as:

Single order of Rs. 250 Crore or more;

OR

Two orders each having minimum of Rs. 156 Crore or more;

OR

Three orders each having minimum of Rs. 124 Crore or more

Similar Projects: - Setting up of Data Centre (including computing, storage & networking Infrastructure) / Operation & Maintenance of Data Centres / Large IT networking/ Network Operation Centres/ Security operation centres/ Smart City Projects.

5. In above orders {(in clause- A (4))}, at least one order should contain Supply & successful implementation of IT Equipment (similar to BoM of this Tender i.e Server, Storage, Networking and firewalls equipment etc.) in Data Centre environment of value not less than Rs. 80 Cr. in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India. *In case of supply of IT equipment in Data Centre project is a part of larger project then bidder should get certificate from Statutory Auditor/Practicing CA regarding value of IT Equipment at Data Centre supplied and installed.*
6. Bidder should have experience of successful implementation of Supply & Installation at 100 locations, of WAN setup, in customer office premises in single or multiple orders *in*

Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.

Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Purchase Order of customers/Clients & Completion date/date(s) should be in between 01/09/2015 to 31/08/2022.

7. Bidder should have its own office at following cities:
 - i. Mumbai
 - ii. Chennai
 - iii. Delhi/Noida/Gurgaon/Faridabad/Ghaziabad
 - iv. Kolkata
 - v. Bengaluru
 - vi. Chandigarh/Mohali
 - vii. Guwahati

An undertaking to this effect must be submitted by Bidder along with details of office address of each location. Detail shall contain, Office address, Contact no. email ID, Office incharge etc. In case, Bidder doesn't have office at any of the above location, A declaration shall be given by the bidder to open the office within 60 days from the date of issue of Contract.

8. The bidder must be an authorised representative of the products/Equipment(s) offered. The authorisation letter from the OEM must be submitted along with the bid **Authorisation** must be issued by OEMs Authorise signatory. **OEMs MAF should contain mainly the following points in its MAF (Manufacturer Authorisation Form) while issuing to bidder:**
 - a) Offered equipment(s)/Software(s) should not be declared end of life/support till 31.12.2028.
 - b) Offered equipment(s)/Software(s) should not be declared end of sale before installation.
 - c) Offered equipment(s)/Software(s) are IPv6 ready.
 - d) Make and Model of Offered equipment(s)/Software(s).
 - e) Equipment(s)/Software(s) supplied by the OEM should be transferrable to any other government agency at a later date along with warranty.
 - f) An assurance from OEM that in case <name of the Bidder> is not able to fulfil its obligation in respect of Warranty, the OEM will continue to meet the warranty terms as prescribed in the Tender document towards ERNET India/CERT-In.

Additionally, in respect of Intelligent Cabling, OEM shall give a certificate that their cabling infrastructure shall have the warranty for 25 years.

9. Bidder should have & provide a dedicated/Toll free no. for service support. *Relevant details to be submitted with Bid Document.*

10. Malicious Code Certificate:

Bidder should upload following certificate in the bid: -

- a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to: -
 - i. Inhibit the desires and designed function of the equipment.
 - ii. Cause physical damage to the user or equipment during the exploitation.
 - iii. Tap information resident or transient in the equipment/network.
- b) The entity will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

B.Original Equipment Manufacturer (OEM)’s Criteria

1. OEMs whose products have been offered in the bid shall have Technical Assistance Centre (TAC) in India. OEM shall have dedicated / Toll Free Number for TAC to support the equipment. OEM(s) should have direct presence with their own office in India. *Relevant documentary proof (i.e. Registration/Incorporation Certificate, Self-certification of TAC availability and Dedicated/Toll free number) should be submitted.*
2. The minimum annual average financial turnover of the each of the following equipment(s) OEM during the last three years (FY,19-20,20-21, 21-22), should not be less than as tabulated below. *A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.*

Sl. No.	OEM of Equipment	Annual Average Turnover (FY 19-20,20-21, 21-22)
1	Servers	850 Cr

3. OEMs shall not be debarred/blacklisted/suspended by Government. A self-declaration to this effect from respective OEMs shall be required to submitted by the bidder at the time of submission of bid.
4. The product (same or similar type as per BoM) offered by OEM should have been supplied and installed (as listed below in last five years) to any Central/State Government/ Govt. undertakings / UT’s/ Autonomous Bodies/Public Listed Companies/ Reputed Private Organisations in India from 01/08/2017 to 31/08/2022. *Copies of relevant documents in this regard should be submitted to the satisfaction of ERNET India.*

Item	OEM should have supplied and installed a minimum of	Unit
Servers	400	no.
L3 Switch	13	no.
Spine Switch with 100G port	1	no.
L3 Switch with 10G/25G/40G/100 G Ports	75	
Routers with at least 50 Gbps throughput	1	no.
Routers with at least 1 Gbps throughput	100	no.
NDR minimum throughput of 5 Gbps	2	no.
IDS/IPS minimum throughput of 2 Gbps	2	no.
Firewall minimum throughput of 100 Gbps	2	no.
AAA Appliance	2	no.
Active Directory Solution	2	no.
SSL VPN Gateway	2	no.
Load Balancer	1	no.
Fireproof Vault	2	no.
KVM Console	20	No.
Degausser	3	no.
Intelligent Cabling & Automated Infrastructure Management	2	Two project of Intelligent Cabling& AIM should be completed.
EMS	4000	Nodes/devices managed in one single project
DCIM	2000	IT/IoT , Non IT nodes in one single project
RF Id based Physical Asset Tracking Tags (rack level Tracking),RF Id Based Heat and Humidity Sensors Tags and RF Id Rack Identifiers	1000	Tags, Sensors, Identifiers
Smart Single Rack (minimum usable space 24 U or more)	5	Smart Racks
Data Diode	5	no.
Laptop	50	no.
Desktop	50	no.
Privileged Access Manager	1000	Node, users

5. The Make & model of the IT equipment offered in bid should be listed (along with Data Sheet) on the OEM website. *Relevant details shall be submitted with bid.*

6. Malicious Code Certificate: OEMs should upload following certificate in the bid: -

This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:

- a) Inhibit the desires and designed function of the equipment.
- b) Cause physical damage to the user or equipment during the exploitation.

- c) Tap information resident or transient in the equipment/network.
7. While quoting the equipment(s) in Bid, Bidder shall make sure following in respect of OEMs
- a. All offered/quoted Servers should be from same OEM.
 - b. All Networking equipment(s) and its transceivers should be from same OEM. Name of such equipment(s) are Spine & Leaf Switch, OOB Switch, Interconnect Type1 & Type 2 Switch, Border Leaf Switch, WAN Switch, DC Routers and Remote Routers cum Firewalls.
 - c. OEM of Internet Firewalls at DR (in HA mode) should be different from the other two types of Firewalls (Internal Firewall & Solution / Application Firewall).
 - d. OEM of Internet Firewalls should be from different vendor.
 - e. There should be only one single OEM of Data Center Infrastructure Management (DCIM), Rack level Live RF Id Based IT Physical Assets Tracking (RLPAT) Solution, Heat and Humidity Sensor based Solution.
 - f. Other line items which are more than one in quantity should be from same OEM line item wise.

Section VII: Scope of Work

1. Project Overview

ERNET India has been entrusted a project by Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology Government of India to achieve the following outcomes:

- i. To setup & Integrate IT Infrastructure and commissioning of Monitoring and Management software at DC , its DR and 250 remote locations.
- ii. To Facilitate installation of third party Operating System and applications on the commissioned computing Infrastructure.
- iii. To Establish MPLS connectivity at DC, DR and 250 remote locations
- iv. To Establish IPsec tunnels over MPLS so as to create data path between commissioned remote sites & Data Centres in order to receive metadata from remote locations to Data Centres.
- v. O&M of supplied Infrastructure and MPLS Links

1.1 Other Tenders Floated for the Project

In order to successfully accomplish the objectives of this project, ERNET India and CDAC have already floated the following tenders:

1. Procurement of IT equipment(s) for 18 remote sites - GEM Bid Number: GEM/2022/B/2381749 : Floated by ERNET India. *For the limited purpose of this tender, the IT infrastructure referred in 1.1 (1) has been referred to as '18 remote sites' in this tender.*
2. To establish core networking infrastructure at DC & 15 remote locations - GEM Bid number# GEM/2021/B/1539956: Floated by CDAC. Currently, this is under installation at this stage.
3. CDAC also procured GEM/2020/RA/57224 & through CPPP portal CDACT.TP.PHS.CSG019D.52.20-21 150 Servers spread in Data Center and remote locations
For the limited purpose of this tender, the IT infrastructure referred in 1.1 (2 & 3) above has been referred to as 'Phase-1' in this tender.
4. To Establish MPLS connectivity - GEM Bid Number: GEM/2022/B/2254639: Floated by ERNET India.

2. Overall Deliverables of Contractor

The overall deliverables of the Contractor/System Integrator (SI) to be selected under this tender are as follows:

- i. Submission of HLD , LLD & site survey reports of DC, DR and 232 remote locations.
- ii. Supply, Installation, Testing & Commissioning of IT Infrastructure and Monitoring and Management software at DC , DR and remote locations as specified in this bid.
- iii. Integration of:
 - a. supplied infrastructure at DC, DR and remote locations as per finally accepted HLD & LLD .
 - b. supplied infrastructure with Phase-1 infrastructure.
 - c. supplied infrastructure & Phase-1 infrastructure with Monitoring and Management software.
- iv. Support the installation of third party Operating System and applications on the commissioned computing infrastructure.

- v. To configure MPLS WAN links & IPSec Tunnels at 250 remote sites & Data Centres.
- vi. Training & certifications as specified by ERNET India in this tender.
- vii. Acceptance Testing as specified by ERNET India in this tender.
- viii. Operations and Maintenance (O&M) of supplied equipment & Phase-1 infrastructure, including supply of manpower for a period of one year at Data Centre (DC & DR).
- ix. Any other electric/networking accessories related work required for installation/commissioning of equipment(s)/software.
- x. Any other activity essential or incidental for successfully accomplishing the objectives & outcomes of this project.

Note1: It may be noted that the Operating System and other core software applications in servers to be supplied under this tender, shall be deployed by empanelled agency of CERT-In, however the servers will be required to be made ready by contractor to enable installation of Operating system and other relevant applications/software on servers.

3. Roles and Responsibilities of Contractor

3.1 Submission of HLD, LLD & site survey reports of DC, DR and 232 remote locations.

- i. Contractor shall carry out necessary site inspection to identify & prepare itself for the required pre-requisites at DC, DR and remote locations for overall smooth installation and commissioning of entire hardware. The contractor is also required to submit the site survey reports of DC, DR and 232 remote locations as per Delivery Plan.
- ii. The Contractor is required to prepare detailed deployment plan along with HLD, LLD and shall submit the same for approval within 10 weeks from the signing of the contract Agreement.

3.2 Roles and Responsibilities of Contractor under this tender & Interlinkages with Other Tenders Floated for the Project:

Contractor of this tender should coordinate with the selected system Integrators / Contractors chosen in the bids mentioned under sub-section ***“Other Tenders Floated for the Project”*** to perform:

- i. End to end integration of all infrastructure procured, including
 - a. Phase-1 IT infrastructure (i.e. Networking, Security appliances & Servers) at Data Centre
 - b. 15 remote sites of Phase-1.
 - c. 30 leaf switch lying with customer extra at DC. Same shall be configured/reconfigured as per requirement
- ii. Synchronize the delivery plan at sites/location with MPLS service provider for ensuring timely end-to-end IPSec Tunnels over MPLS from all sites/locations.
- iii. O&M of Phase-1 infrastructure.
- iv. Coordination with Contractor of ***‘18 remote sites’ for driving the activities of scope of work or O&M etc. Further, it is clarified that O&M activities for ‘18 remote sites’ is not in scope of this tender.***

4. Role and Responsibilities of contractor at Data Center:

It must be noted by Contractor of this bid that 32 networking and server racks are under installation at the DC and contractor needs to understand HLD and LLD of existing IT infrastructure of Phase-1 Data Centre so as to ensure that the expansion of DC with equipment supplied in this bid is carried out seamlessly. Following are the broad list of roles and responsibilities of the contractor of this tender:

- 1) Perform the Site Survey and submit the survey report along with the HLD & LLD.
- 2) Supply of equipment & related software as per specification & BoM at DC and the installation, testing, commissioning & configuration of all supplied equipment(s) & software at DC . Integration of all remote sites through IPsec over MPLS Links.
- 3) Expand and Integrate the existing IT infrastructure of Phase-1 Data Centre with the equipment (s) planned in this tender utilizing the existing HLD and LLD.
- 4) To provide necessary support for the installation of third party Operating System and software applications on the commissioned computing infrastructure.
- 5) Coordinate with other SI(s) for MPLS link(s) availability
- 6) Integration of '**18 remote sites**' & **additional '15 remote sites' of Phase-1** with DC.
- 7) Installation, Commissioning and Integration of AIM (Refer section "Integration with existing AIM at DC) , EMS, DCIM, & other relevant software with complete IT infra. Refer to their integration in respective sections of this tender document.
- 8) Setup of High Availability Modes of operation for the equipment(s) & software at DC as per specification .
- 9) Contractor will update the configuration of the networking equipment(s) as required by CERT-In/ERNET India.
- 10) Contractor shall configure all the components and sub-components for end-to-end user access to all applications/services.
- 11) Training on the infra and software installed via this tender & certifications as specified by ERNET India in this tender.
- 12) Perform the security audit (including VAPT) and fix all security issues at the time of acceptance.
- 13) Acceptance testing as specified by ERNET India in this tender.
- 14) Operation & Maintenance (O&M) for one year after successful implementation and acceptance by ERNET India including O&M for existing equipment(s) of Phase-I.
- 15) Supply of requisite manpower as per specifications.

5. Role and Responsibilities of contractor at Disaster Recovery Data Center (DR):

Contractor will be required to perform the following activities to setup DR of the above mentioned DC as specified in this tender:

- 1) Site Survey, and Preparation of High Level Design & Low Level Design for DR in sync with DC. Submission of Survey reports and design. The architecture in DR would follow the same design and functional principles as laid down for DC . Contractor to ensure for smooth integration/functionality of various analytics application and tools across DC and DR.
- 2) Setup of Cabling structure at DR similar to as described for DC . The fiber pathway will already be installed at DR. These Pathways shall be suspended from the ceiling at above the rack height.

- 3) Supply of equipment & related software as per specification & BoM at DR and the installation, testing, commissioning & configuration of all supplied equipment(s) & software at DR . Integration of all remote sites through IPsec over MPLS Links.
- 4) To provide necessary support for the installation of third party Operating System and software applications on the commissioned computing infrastructure.
- 5) Coordinate with other SI(s) for MPLS link(s) availability
- 6) Integration of '**18 remote sites**' & **additional '15 remote sites' of Phase-1** with DR.
- 7) Configuration of equipment(s) to establish interconnectivity and integration of DC with DR .
- 8) Installation, Commissioning and Integration of EMS, DCIM, AIM & other relevant software. Monitoring & Management of services and equipment through Hardware & software procured in this tender.
- 9) Establish Automated Infrastructure Management (AIM) solution at DR in line with DC for monitoring of all racks which will be around 60. Integration of AIM with DCIM & NMS as per tech specs.
- 10) Setup of High Availability Modes of operation for the equipment(s) & software at DR as per specification .
- 11) Contractor shall configure all the components and sub-components for end-to-end user access to all applications/services.
- 12) Contractor will provide Operation & Maintenance for supplied equipment/software at DR for one year after its successful implementation and acceptance by ERNET India.
- 13) Contractor will update the configuration of the networking equipment(s) as required by CERT-In/ERNET India.
- 14) Training on the infra and software installed as specified in this tender .
- 15) Perform the security audit (including VAPT) and fix all security issues at the time of acceptance.
- 16) Acceptance testing as specified by ERNET India in this tender.
- 17) Supply of requisite manpower as per specifications.

6. Role and Responsibilities of contractor at Remote Sites & its Integration

Contractor will have following roles and responsibilities for the remote sites :

- 1) Site Survey and Submission of Survey Reports of 232 remote sites.
- 2) Preparation & Submission of High Level Design & Low Level Design to be followed at remote sites.
- 3) Supply of equipment & related software as per specification and BoM at 232 sites and installation, Testing, Commissioning & Configuration of all supplied equipment(s) at 232 remote locations.
- 4) Integration of equipment(s) with MPLS Links and data path establishment with Infra at Data Centers (DC & DR) via IPsec tunnels between commissioned remote sites & Data Centres (DC & DR) in order to receive metadata from remote locations to Data Centres and established secured IPsec Links for data communication.
- 5) Management and Monitoring of services and equipment through software procured in this tender.
- 6) SI needs to coordinate with Contractor of '18 remote sites' tender to ensure that these '18 remote sites' are well integrated over MPLS via the IPsec tunnels with the DC and DR.
- 7) Configuring/Integrating the Management and Monitoring software at DC and DR with all remote sites including '15 remote sites' of 'Phase-1'.

- 8) Configuration to establish data communication of remote sites with DC or DR based on link availability at DC and DR..
- 9) Perform the security audit (including VAPT) and fix all security issues at the time of acceptance.
- 10) Operation & Maintenance for one year after successful implementation and acceptance of services & acceptance by ERNET India.

7. Role and Responsibilities of Contractor i.r.o EMS, DCIM and related software applications:

- 1) Setting up, configuring and integrating requested software modules such as AAA, Active Directory, EMS, AIM, DCIM, IT Helpdesk, Asset Management etc. (its complete list as per BoM & specifications) in a High Availability (HA) mode for administration, monitoring and management of infrastructure and established Network. EMS OEM holds the responsibility to must perform integration of overall EMS solution & DCIM (with all their respective sought modules). Contractor must ensure that the integration of EMS with all IT equipment procured via
 - a. 'Phase-1' tender ,
 - b. '15 remote sites' of Phase-1,
 - c. '18 remote sites' tender
 - d. Equipment supplied as a part of this bid. Contractor must ensure that all this equipment is discoverable and manageable via the EMS.
- 2) Installing & configuring AAA server & Integrating AAA within the setup for required functionalities such as authentication of all users, logging of session information/details pertaining to NEs, tracking of sessions, logging of configuration changes per user , enforcing security policies on the end network elements etc.
- 3) Installing & configuring Active Directory (AD) for setting up users with different roles/privileges to allow privileged access to different modules , setting up user-privilege based different workflows for change management / configuration changes etc.
- 4) Accordingly, the contractor should ascertain any other requirements such as configuring DNS /DHCP etc. w.r.t full functioning of AD/AAA.
- 5) Installing & configuring AIM solution at DC and DR. Integrating new & existing AIM solution at DC with EMS. Integrating AIM solution at DC and DR with EMS.
- 6) Deployment and Integration of RF based Physical Asset Tracking, Heat and Humidity Sensor Solution with DCIM at DC and DR.
- 7) Integration of DCIM and EMS using REST APIs/SNMP and / or any other available non –proprietary interfaces available for integration between modules for accomplishing requirements and complete functionality.
- 8) Installation, configuration of a syslog server, its integration with EMS and integrating it with all network devices & servers to aggregate syslog(s) at this server.
- 9) Data & Module wise Integration:
 - a. RF based Physical Asset Tracking solution should be able to route the relevant data to DCIM and then to EMS by forwarding SNMP traps and/ or the relevant data e.g. Alarm(s) generated via an unauthorized movement of asset should be sent to EMS or any other alarm generated w.r.t Asset Management Functionality should visible in EMS alarm module and EMS database. Further, such an alarm in EMS should auto raise a ticket in IT helpdesk (based on certain criteria). The ticket may be closed by a user by referring / adding remarks to the ticket id w.r.t a ticket generated for authorized movement of asset as above. The alarm may be also acknowledged with this ticket id.

- b. Another such desired required integration is to move an asset from a Rack to another Rack in the IT Helpdesk system, this will be tracked via a ticket. Any change needs to undergo via change management workflow , which means this request will be reviewed and approved by different users. Upon approvals a change becomes an authorized change.
- 10) The Contractor needs to create processes and perform required integrations to accomplish the functionality.
 - 11) Installation and commissioning of IP Address Management and Switch Port Management solution along with the EMS so as to allow advanced IP scanning of IPv4 and IPv6 subnets in network for identifying the available and used IP addresses. i.e. it must support Network inventory management with IP address and Switch port management.
 - 12) Setting up / configuring SLAs per device/logical device / link basis and as desired in tender SLA conditions and provide the detailed weekly/ monthly downtime using tools (if any tool than supplied EMS is used, contractor needs to provide the same as well). Provide root cause analysis for the alarms etc. contractor needs to configure the SLA management module as per the SLA/penalty terms and conditions mentioned in the tender. contractor needs to ensure that SLA module is able to generate the report with penalty details based on the downtime as per conditions mentioned in tender.
 - 13) Configuring Drawings , Photos & Videos of Floor(s) of DC , DR and Building Layout in the DCIM and / or EMS.
 - 14) Integration of DCIM with all RACK's PDUs at DC and DR.
 - 15) Integration with Email Gateways/servers, SMS Gateways.
 - 16) Integration of DCIM with BMS is in the scope of Contractor, provided the BMS supports and provides the requisite APIs.
 - 17) In order to complete the solution and scope of work, contractor needs to provide and configure OEM's MIBs for IT equipment (servers, networking equipment etc.), OEM's Element Management Systems (Networking, Server equipment and all other possible IT equipment) and perform the end to end integration of EMS with OEM's Element management systems for the completion of the requirements. e.g. Element Management system is required to monitor and manage the alarms / events pertaining to fan, physical ports etc. Hence , for such alarms/events/traps based integration, Contractor must provide the relevant source MIBs from OEM. Contractor must ensure the Element Management Network's integration with EMS(Enterprise Management System) .
 - 18) Contractor must provide & configure CA certificates from Verified CA store to allow both Internet and Intranet Access to software web based modules (such as EMS/DCIM etc.) which are valid for the total duration of work on all **applicable** devices/servers to support SSL based encryption. The default access to EMS and other management modules provided should be via only Intranet, whereas in certain special cases, internet access to specific modules may be provided upon authorized requests& approvals in system (Helpdesk).
 - 19) Deployment of relevant applications/ software modules for EMS and DCIM solutions should be on different physical servers. The requisite modules should be integrated as per specifications on Day-1. There should be seamless automatic successful handover (in failure cases) between the instances provided in HA. Refer Technical specs for more details. Contractor must also create and provide the SOP to be followed whenever any instance / instances goes down.
 - 20) It is responsibility of contractor to maintain the backup of EMS for at least one year which includes data, configuration, alarms, performance etc. Assets data must be maintained throughout.

- 21) Contractor may choose the best and optimized design to deploy the various sought applications / solutions on Hardware. The contractor must ascertain the hardware & other requirements of these servers as per the sought criticality, HA, scope of work, total users, backup , total concurrent users, amount of data to be saved per server per application and other factors.
- 22) Contractor is responsible to offer complete hardware and software to run the applications and monitoring of equipment and appliances mentioned in the BoM along with the equipment procured under different bids referred in this document. The Contractor must ensure automatic sync up of data related to EMS & DCIM applications between various instances under different fail over scenarios.
- 23) Maintain backups of all the versions of equipment software, configuration user details, log details etc. Contractor shall perform proper version management of all the equipment configurations. All the changes must be formally approved by the ERNET India/ CERT-In designated team leaders and recorded as per process.
- 24) Contractor shall ensure that these backup and configurations are accessible only to the authorized person and must be kept with the ERNET India/ CERT-In and designated in-charge as per Information security policy of ERNET India/ CERT-In.
- 25) The Contractor shall ensure that all the devices that will be installed in the DC, DR , remote locations as part of the physical infrastructure shall be Simple Network Management Protocol (SNMP) latest version enabled and shall be centrally monitored and managed on a 24x7 basis.

8. Role and Responsibilities of Contractor i.r.o Integration of DC equipment(s) with Phase-1 IT equipment(s):

- 1) CERT-In is in the process of setting up of Networking, Security & Servers etc. through another Contractor in approximate 32-34 Racks. HLD & LLD of DC i.e. phase-1 IT infrastructure will be provided to Contractor, Contractor needs to align themselves according to HLD & LLD to extend the DC with the IT Infrastructure of this tender. List of available equipment(s) with Make & Model shall be provided to prospective Contractors on submission of Non-Disclosure Agreement.
- 2) Contractor shall perform SITC of the IT equipment(s) and software planned at DC in this bid and integrate with the already existing equipment(s) of phase-1.
- 3) The existing Data center is under implementation with open standards Leaf and Spine architecture. The Additional Leaf Switch procured through this tender must be fully integrated with existing Spine Switch of phase-1 to make it a part of existing DC Fabric. These new leaf switches should be seamlessly managed by existing controller. This is to ensure that the New and existing networking environment of Data Center works as a single unit and can be used seamlessly.
- 4) The Integration of the existing DC with extension of leaf switches is very critical. The existing DC will be made up soon and the extension of the OOB and leaf's Switches should not affect the existing DC architecture, traffic flow, performance, resiliency, overlay, underlay etc. The Contractor needs to perform PoC (proof of concept) as per requirement in existing DC to confirm single fabric unified architecture along with security and Routing functionality desired.
- 5) The Contractor shall integrate EMS (i.e. in this bid), DCIM and remaining software with existing equipment installed and commissioned in phase-1, by referring to this bid's technical specs, scope of work and sought functionality.

- 6) At present 32 remote locations planned to be connected through IPSec tunnels to the available WAN Switch and CE Router at Data Center. New 232 remote locations will also be connected through these existing equipment (s) in same manner.

8.1 Integration with Phase-1 Intelligent Cabling Infrastructure at Data Center:

ERNET plans to expand an existing data center with additional 70 (seventy) Server Racks (S/R). The 70 S/R are to be seamlessly integrated with the existing data center. This would include integrating the complete passive structured cabling solution (copper & fiber) and the Automated Infrastructure Management (AIM) solution currently under installation in the existing data center. The existing data center would approximately consist of 30 (thirty) S/R and 2 (two) to 4 (Four) Network Racks (N/R). The following sections will detail the Scope of Work (SoW) that needs to be fulfilled for a seamless integration of all areas. List of available equipment(s) with Make & Model shall be provided to prospective Contractors on submission of Non-Disclosure Agreement.

8.1.1 Integration with existing Passive Structure Cabling at DC:

- 1) The passive structured cabling design that is to be deployed in the additional 70 S/R will follow the same design that has been planned to implement in the 30 S/R for the existing data center. Refer to Phase-1 Networking Infrastructure description in Technical Specification under Data Center Intelligent Cabling section for more details.
- 2) All structured cabling products proposed shall be governed by the Technical Specifications listed in this tender. All copper and fiber panels shall be intelligent enabled from Day 1. The existing data center uses standard based patch cords and the same shall be the case for the additional 70 S/R.

8.1.2 Integration with existing AIM at DC:

The Automated Infrastructure Management (AIM) solution proposed by Contractor for the 70 S/R shall seamlessly integrate and shall be interoperable with the existing AIM solution and work as a single entity. All 70 S/R shall be intelligent enabled where all the connectivity within the rack shall also be monitored via the AIM system. The AIM solution shall monitor the complete connectivity between N/R racks and S/R racks; therefore, the software shall provide the complete end to end circuit trace (including the active equipment port) between N/W and S/R on the same window and shall also appear on the rack controller when prompted physically from the rack. The integration shall be such that only a single web-based window should be required to monitor both the existing AIM software and the proposed AIM software. The proposed AIM solution shall have the following features that are currently available/functioning on the existing AIM solution. (refer to detailed feature specification has been provided in the Technical Specifications). The AIM Software shall have the capability to select the endpoints of the circuit and let the AIM Software automatically identify the patch connections, available routes necessary to complete the circuit.

- 1) The AIM Software shall have a dashboard feature which allows various types of indicators to be viewed and monitored. Some mandatory indicators that shall be part of the AIM

software are, total fiber and copper panel ports in use, total space utilized in a single rack, total fiber and copper switch ports in use, total fiber and copper server ports in use.

- 2) The integration of existing and new AIM with EMS for the Alarms or any other events.
- 3) In case Contractor proposes cabling from existing OEM in this bid, the Contractor may use existing AIM Hardware and Software with extra licenses as required, provided there are no constraints on performance. In case of any scalability/performance issues envisaged with existing AIM Hardware and/or Software, the Contractor may provide the relevant and appropriate AIM Hardware and / or software with required licenses.

9. General Activities to be performed by Contractor for the project: -

- 1) The tasks under SoW are to be performed by selected Contractor of this bid in coordination with respective OEMs/vendors, MPLS Bandwidth service provider, existing Contractors, ERNET India, CERT-In and other agencies relevant for this project.
- 2) Define processes (SOP) such as for IT equipment & their security Policies, defining the security plan for audits, other processes such as for SITC and O&M of IT equipment, it should also include unloading of assets, placement as inventory, unpacking, addition of asset tags on inventory, installation, commissioning and its discovery in EMS. The SOPs should include the scenarios of Asset movement, configuration, reconfiguration of asset tags for new location with proper documentation and reporting etc.
- 3) Define and document the processes for various activities to be performed such as Pre-Installation, Installation-Configuration-Commissioning, Coordination with other Project Vendors processes etc.
- 4) Documentation of implementation procedures/guidelines and workflows for processes/ use cases manually/automatically identified. Revise and re-issue of such guidelines / procedures based on feedback during O&M period.
- 5) Create and manage a project documentation library containing the project documentation templates and ensure continuous process improvement for the project under knowledge management.
- 6) Contractor shall suggest a change management process based on the network, systems, solutions and applications deployed. It must help to create the workflow templates, define the users and their access roles.
- 7) Contractor adhere to the change management procedures already defined (if any) in ERNET India/CERT-In policies to ensure that no unwarranted changes are carried out on the devices.
- 8) Training of ERNET India and CERT-In manpower about installation and operation of equipment(s).
- 9) Contractor shall have proper escalation procedure and emergency response for any failure of DC and DR.
- 10) Since the project is being implemented in a secured environment, all the updates/patches of the devices and software solutions shall be performed without direct connectivity to Internet. The updates/patches files should be download offline in an independent system, from where in-turn USB/portable HDD based updation /patching etc. is carried out to periodic & on-demand mechanism.
- 11) Contractor to ensure that Servers are supplied along with all the necessary drivers to run Operating systems as mentioned in technical specification.
- 12) The bid should include OEM professional services for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with

expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.

- 13) Any other activity essential or incidental as decided by ERNET India during the project period as per the scope of work and technical specifications.
- 14) Any other essential or incidental work required to be performed by the contractor to commission the project.
- 15) **Processes & Guidelines:** The Contractor must create and develop the relevant processes for the project implementation phase and get those approved from ERNET India. These must be (version) maintained and saved in knowledge management database.

10. Acceptance Testing (AT)

- 1) The draft Acceptance test plan (ATP) with detailed procedure shall be submitted by Contractor within eight (8) weeks of issuance of Contract for review and approval by ERNET India /CERT-In. AT shall be carried out jointly by Contractor and ERNET India/CERT-In after successful delivery, installation, testing and commissioning of project as per milestones. On successful completion of AT, certificate for the same shall be issued by ERNET India to the Contractor. Operation and Maintenance of individual milestone will start from the date of acceptance by ERNET India. Responsibility of Contractor shall include below mentioned artefacts but not limited to:
 - a) Submission of ATP document.
 - b) OEM(s) Certification for installed equipment(s) as per the best practices and guidelines with requisite quality as per OEM standards.
 - c) Low level and High level design and Network security policy document.
 - d) All equipment(s) and software items must be installed at site as per the specification and establish of transfer of data between central and remote sites through IPSEC tunnel.
 - e) Availability of all the defined services shall be verified.
 - f) Successful Vulnerability assessment (VA) and Penetration Testing (PT) report through a Third-party certified agency (CERT-In empanelled Security auditors) and Fixing of all identified Vulnerabilities upon upgrades/patch updates and providing the “all clear” reports.
- 2) ERNET India may require the Contractor to carry out any test and/or inspection not specified in the Contract but deemed necessary to verify that the characteristics and performance of the equipment(s) and services comply with the technical specification’s codes and standards under the Contract. The Contractor shall be required to carry out such test and/or inspection at its own cost.
- 3) Final Acceptance for each of the milestone in the project will be given by ERNET India along with CERT-In.
- 4) Any other document/activity identified during project implementation period.

11. Training

The Contractor must conduct training for users (ERNET India/CERT-In officials) for all technical and operational aspects of the equipment and services such as Servers, Router, Switches, Firewall, EMS, DCIM etc. The training may happen for multiple people at multiple times. The Contractors has to coordinate with ERNET India/CERT-In to finalize a training calendar, get the same approved and adhere to timelines. The training must take place before the handover of the Milestone-1.

- 1) Training for 50 Persons shall be provided onsite by the Contractor or Contractor's representatives / respective OEMs for a minimum period of 30days for installation and operation of installed equipment(s).
- 2) The training should comprehensively cover all the supplied sub-systems, their integration and operations. Including
 - i. Installation of all hardware and software.
 - ii. General system administration, maintenance & operations.
 - iii. Installation, configuration and administration of all Networking, Firewalls, Servers, AAA Appliance, Load Balancer, NDR, EMS, DCIM, CMS, IT Helpdesk etc.
 - iv. Installation & configuration of all software items supplied.
 - v. Performance analysis & tuning.
 - vi. Problem diagnosis, pre-failure alerts, logs management, reports, and problem resolution.
 - vii. LAN, WAN, network and security devices.
 - viii. All supplied software including server & storage management software, EMS, Anti-virus software, etc.
- 3) Comprehensive hardcopy and soft copy training course material must be provided.
- 4) The documentation including the presentations/write-ups / notes must be arranged and saved in the knowledge repository (Onsite only).
- 5) Contractor shall also provide following Training & budget for the following certifications:

	Training Detail	No. of Staff
Training & certification	Professional Level Proficiency Certifications equivalent to CCNP, JNCIP for Data Center, Routing and Switching, Security and LPIC1 & LPIC2 for Linux Administration	
	1. Data Center	30
	2. Routing and Switching	35
	3. Security	35
	4. Linux System Administration	30

12. Scope of Work for Operation and Maintenance

The Contractor shall carry out operations, maintenance and management of all installed IT components(Hardware and software) immediately after acceptance of each Milestone by ERNET India/CERT-In and also provide Comprehensive On Site maintenance of equipment installed in DC, DR & remote Sites for a period of one year. The minimum

specified work to be undertaken by the Contractor for providing operations, maintenance and management of all IT components & comprehensive onsite maintenance during the contract period has been categorized as under:

- 1) Operations, maintenance and management of all IT components(Hardware and software) and related services for the equipment installed as per BoM at DC, DR & Remote sites.
- 2) Comprehensive Onsite Maintenance with spare parts for all equipment's/items mentioned in BOM.
- 3) Operations, maintenance and management of all IT components and related services for the Phase-1 equipment(s). List of available equipment(s) with Make & Model will be provided to prospective Contractors after submission of Non-Disclosure Agreement (NDA). These equipment (s) are under warranty. Extension of warranty/AMC of such equipment are not under purview of this tender.
- 4) Keeping the warranty of supplied hardware in this bid & other existing hardware of Phase-1 intact will be the sole responsibility of successful Contractor.
- 5) Maintain helpdesk and do follow-up with other Contractor for existing equipment and bandwidth service providers in case of faults during O&M period.
- 6) Contractor shall carry out Vulnerability assessment (VA) and Penetration Testing (PT) using certified tool through a Third-party certified agency certified by CERT-In of complete IT infrastructure once in a year and shall submit report to ERNET India/CERT-In.
- 7) During the O&M period, the Contractor shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 15 days of their availability/release and should carry out installation and make operational the same at no additional cost to ERNET India/CERT-In. Contractor must ensure that permission has been taken from ERNET India/CERT-In before any updates, patches/fixes, and version upgrades.
- 8) Generation of analytical reports on daily, weekly, monthly basis and submitting to ERNET India/ CERT-In for reviewing.
- 9) Review meeting shall be held weekly and monthly during O&M period.
- 10) Processes & Guidelines:
 - a. The contractor must create and develop the relevant processes for the project O&M phase and get those approved from ERNET India /Cert-In
 - b. Some of the processes include change in configuration/IP addresses / user management (users/privileges) / WAN network / IPSec tunnels/Local Network/asset locations/link parameters/threshold.
 - c. Contractor must provide the O&M plan including the periodicity of submission of required artefacts / documents.
- 11) **Reports:** Contractor must provide
 - a. Regular weekly & monthly reports for the alarms / incidents reported.
 - b. Regular monthly reports for
 - i. SLA calculations, Inventory and Assets, Availability of Manpower
 - ii. Open / Closed / In Progress Helpdesk tickets, Feedback , Root causes of regular alarms/problems, Improvement areas.
 - iii. Contractor shall undertake proactive monitoring of the entire basic infrastructure and diagnose problems that could arise as part of any component installed in DC, DR and remote locations. Contractor shall maintain a log of all such diagnosis and notify ERNET India/ Cert-In on a monthly basis in the form of a report.

- iv. Other reports planned and discussed during the course of project.
- 12) Contractor must ensure the following at all times, during implementation:
 - a) Availability - All components must provide adequate redundancy to ensure high availability of the applications, devices and other DC & DR services. Designed IT infra shall have ability to withstand all single point of failure without any service unavailability.
 - b) Lean and Clean Design –SI must follow the recommended measures for a lean and clean design – e.g. structured cabling for the DC & DR infrastructure etc.
 - c) Scalability & Flexibility
- 13) Any other activity which may be mutually decided during the contract period.

The following are the other major activities to be carried out for the equipment/software/services installed or to be installed in DC, DR & Remote Sites during the contract period.

12.1 Asset Management Services

The Contractor shall be required to create and maintain database of all the assets installed/procured/brought by ERNET India/CERT-In in the DC, DR & Remote Sites as per Asset Management policy.

Some of the points are mentioned but not limited to following:

- i. Contractor needs to provide a process for taking in/out of a project asset at a site that should include performing the Asset Tagging for the DC&DR assets and maintaining of asset tags ids per DC & DR assets in DCIM / RF Id Tag solution. The process should include updates in Asset Management Solution.
- ii. The Contractor needs to take an approval for the process established from ERNET India / Cert-In and accordingly create a change management workflow
- iii. Contractor must maintain the asset details of all assets of the project (including the existing & upcoming assets).Old inventory details will be provided by ERNET India. The asset inventory database should have information like make, model, power load, configuration details, serial numbers, EoL, EoS, licensing agreements, warranty/support details, place/location of installation and installation/removal details etc.
- iv. The Contractor shall create and maintain software inventory database with the information such as Licenses, Version Numbers, Support Expiry and Registration details.
- v. The Contractor shall notify atleast 3 months in advance to tendering authority for Hardware and Software warranty/support / EOL contract renewal before.
- vi. Asset Management of any other existing hardware of project shall also be maintained by Contractor.
- vii. Monthly Manual Auditing of DC-DR Assets and crosschecking of same with the Asset details of the system. Documenting and Submitting the reports with gaps found if any.
- viii. Regular reports w.r.t items in staging area, store, racks in DC and DR.
- ix. 100% tracking of all resources of project, ensuring that all items in assets are searchable in asset database by their serial number, IP addresses or other unique fields.
- x. Provisioning of different color labels on to all assets placed in different areas in DC, DR as a staging, store, racks.
- xi. Any other activity which may be mutually decided during the project period.

12.2 Preventive Maintenance Services

The Contractor shall ensure preventive maintenance (PM) services for all the IT equipment installed at the DC & DR at least once in every quarter and for Remote Sites once in a year. The preventive maintenance shall include:

- i. Cleaning and removal of dust and dirt of the equipment with appropriate precautions.
- ii. Bidder must perform the PM inline with the OEM standards or as defined by CERT-In/ERNET India.
- iii. Conduct inspection (check for loose contacts in the cable and connections etc.), health checking of all components of the equipment, testing, satisfactory execution of diagnostics and necessary repairing of equipment.
- iv. Contractor shall intimate and take due approval from ERNET India/CERT-In before carrying out preventive maintenance activity.
- v. Proper labelling/ferruling and dressing of cables, Contractor shall provide labelling/ferruling and commercial label printer, consumables including cartridge, label stickers, cable tie etc.
- vi. Any other activity which may be mutually decided during the project period.

12.3 Installation/configuration and reconfiguration/rollback of equipment

The Contractor shall be responsible for installation/configuration/re-configuration/rollback of all the equipment as and when required by ERNET India/CERT-In.

- 1) The Contractor shall maintain a record of hardware and software configurations of all equipment including the details of different policies/services implemented on the devices such as VLAN configurations, access control lists, routing filters, clustering, versions etc. (except OS & other applications along with Database, Storage etc.).
- 2) Contractor shall keep backups of all the versions of equipment configuration.
- 3) Contractor shall adhere to the change management procedures already defined in ERNET India/CERT-In policies to ensure that no unwarranted changes are carried out on the devices.
- 4) Contractor shall do proper version management of all the equipment configurations. All the changes must be formally approved by the ERNET India/CERT-In designated team leaders and recorded.
- 5) Contractor shall ensure that these configurations are accessible only to the authorized person and must be kept with the ERNET India/ CERT-In and project manager as per Information security policy of ERNET India/ CERT-In.
- 6) Any other activity which may be mutually decided during the project period.

12.4 Network Management Services

The scope of work under network management services would include –

- i. To ensure continuous operation and upkeep of the network Infrastructure at the Data Centres & Remote Sites so that the network is available 24 x7 as per the prescribed SLA.
- ii. Configuration/Reconfiguration/Deployment and Management of various device policies like Security policies, Access policy, IP Policy, routing policy, firewall policies etc. as per ERNET India/ CERT-In requirements.
- iii. Managing accessibility between external links and project infrastructure hosted at the Data Centres in co-ordination with respective vendors.
- iv. Configuration/Reconfiguration/deployment/installation and maintenance of all Network equipment installed or to be installed at the Data Centres & Remote Sites.
- v. Performance tuning to ensure resilient performance, reliability and high availability of the network services. A performance matrix has to be provided by Contractor to the ERNET India/CERT-In on monthly basis and as and when required.
- vi. Coordination with defined agencies for WAN links .
- vii. The Contractor shall also be responsible for integration, management, maintenance, configuration /reconfiguration and commissioning/decommissioning of any additional Internet/Intranet Bandwidth from different ISPs and other department networks which needs to be integrated with DC network during entire contract period.
- viii. The Contractor shall be responsible to monitor the availability of various links and their packet drop, latency and utilization at the DC, DR & remote sites network using EMS. The Contractor shall also maintain logs on the basis of time, interface, IP address, application wise etc. for traffic analysis for the requisite period defined in respective policies.
- ix. Any other activity which may be mutually decided during the project period.

12.5 Server Management Services

The Contractor has to provide these services for supplied servers

- i. Contractor shall manage the server hardware including server hardware installation, POST, administration, hardware performance tuning and upkeep of the server.
- ii. The Contractor shall also undertake installation/re-installation of all the servers in terms of Hardware installation & powered on.
- iii. Contractor shall provide device/peripherals management.
- iv. The Contractor shall be responsible to monitor the availability of various CPU utilization, port status, fan status , latency and utilization at the Data Centres & remote sites servers using EMS/ DCIM. The Contractor shall also maintain logs on the basis of time, interface, IP address, application wise etc. for traffic analysis for the requisite period defined in respective policies.
- v. Collection of sysLogs from all the subsystems, integrated into a Syslog server, sysLog backup as per policy, integration of alerts/alarms / events with EMS.
- vi. Contractor shall be responsible to maintain optimum utilization of all the equipment's w.r.t. keeping close watch on optimum performance of Hardware and implementing necessary measures to rectify the issues using available tools in data centre. A performance matrix has to be provided by Contractor to the ERNET India on monthly basis and as and when required.
- vii. Any other activity which may be mutually decided during the project period.

12.6 Enterprise Management (EMS) & Data Centre Infrastructure Management (DCIM) Services

The objective of these services is to ensure continuous operations and upkeep of the WAN infrastructure at the DC, DR, remote locations including all active and passive components. The scope excludes maintenance of WAN links which shall be the joint responsibility of MPLS Service Provider and ERNET India. However, for overall functioning of the Infrastructure & to achieve the desired project objectives, at optimum performance within permissible SLAs, the Contractor will be responsible to coordinate with MPLS Service Provider for WAN links related issues for integration amongst DC, DR, remote locations.

The scope of work under EMS & DCIM services would include but not limited to: –

- 1) Operations and maintenance of EMS and DCIM installed with its various modules.
- 2) Supplied solution's upgrades, patch updates etc. for the overall contract period via only non-Internet based mechanisms.
- 3) Provide traffic analysis and service management of Non IT and IT (network and server) infrastructure deployed at different physical locations including DC, DR, Remote locations (described as per scope of work and BoQ),18 remote locations (being procured as a part of another bid) and also on already existing equipment of phase-1 containing NEs and Servers at DC location & 15 remote locations.
- 4) Providing preventative maintenance plan, asset audit plan, SOP required for change management workflows and take an approval from ERNET India / CertIn for same and perform the maintenance as per plan.
- 5) Provisioning of regular daily/weekly/monthly reports including but not limited to reports related to Equipment Availability, Link Availability Network based reporting between network devices, VLANs created for various co-hosted users including their traffic analysis. Contractor should provide current and historical reports for various statistics monitored.
- 6) Contractor must Maintain End of Life, End of Support, End of Sale for Assets, trigger early actions (in advance of three months) w.r.t it to ERNET India / Cert-In.
- 7) Bi-yearly audits of assets using 2D barcodes and comparing with Asset management module, presentation of discrepancies, updation of SOP if required, correcting the database . In case any additional equipment/tool is required pertaining to 2D bar code audits, Contractor must take them into account.

12.7 Security Administration and Management Services

The objective of this service is to provide a secure environment in compliance to the ERNET India/ CERT-In security policy. This service includes:

- i. Addressing the ongoing needs of security management including, but not limited to, monitoring, configuration/reconfiguration, troubleshooting of various devices/ tools such as firewall, IPS/IDS, through implementation of proper patches, procedures and rules.
- ii. Ensuring that latest patches/ workarounds for identified vulnerabilities are applied immediately. Contractor shall enforce update/upgrade managements.
- iii. Respond to security breaches or other security incidents by taking corrective measures, providing guidelines to users and coordinate with respective OEM in

case a new threat is observed to ensure that workaround /patch is made available for the same.

- iv. Protection from viruses / malwares etc. is the responsibility of Contractor for the supplied systems. Contractor must provide antivirus / end point protection with regular updates and take sufficient steps to avoid any kind of attack on supplied systems.
- v. Configuration/reconfiguration, Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, firewalls, servers, from viruses.
- vi. Ensuring that the security policy is maintained and updates to the same are made regularly as per ERNET India/ CERT-In Security guidelines.
- vii. Compliance of security regulations defined by Government of India or any other Govt. Authorized agency.
- viii. Report generation

12.8 Disaster Recovery Configuration Services

All the critical applications of DC shall be setup and configured in the Disaster Recovery (DR).

- i. The Contractor shall be responsible for setting up Network services at disaster recovery site for Auto/Manual switch over to run the critical applications from DR in case of any unforeseen disaster at Main DC or as per the directions of ERNET India/ CERT-In.
- ii. Disaster recovery site configuration includes configuration of all IT infrastructures in DC and DR Site and Contractor shall be responsible for configuration, management & Changes of all IT infrastructures i.e. network equipment etc.
- iii. Detailed scope may be worked upon during implementation.

12.9 Network Management Services including Security Incident Lifecycle Management

The objective of this service is to ensure continuous operation and security of the ERNET India/ CERT-In infrastructure at Data Centers & Remote Sites. For overall functioning of the services, the Contractor shall be responsible to coordinate with Bandwidth service Provider team for MPLS link related issues. The services to be provided for Network Management include:

- i. Ensuring that the network is steady and available 24x7x365 as per the prescribed SLAs.
- ii. Attending to and resolving network failures and snags within time limit as defined in SLA.
- iii. Attending to and resolving network security incidents within time limit as defined in SLA.
- iv. Support and maintain the overall network infrastructure Security Components, Switches etc.
- v. Configuration and backup of network & security devices including documentation of all configurations.
- vi. 24x7x365 monitoring of the network to spot the problems immediately.
- vii. Installation and Re-installation of the network devices in the event of crash/ failures.
- viii. Tuning of various parameters to optimize performance and to ensure industry standard QoS with customization is being delivered.
- ix. Any other activity which may be mutually decided during the project period.

12.10 Remote site support

Contractor will have to provide support on remote site for supplied hardware.

- i. Contractor team will monitor the Link/Site status from Data Center NoC.
- ii. Any alert raised for WAN link has to be communicated from Monitoring /Helpdesk team.
- iii. Liaisoning with Bandwidth Service Provider to make the link up 24x7x365.
- iv. Contractor has to ensure the standard warranty support from OEM at sites as well including HW SLA defined in SLA annexure.
- v. All configuration management will be done from DC/DR for supplied devices under this contract.
- vi. Any HW support has to be catered by Contractor on call basis.
- vii. OEM support for HW replacement has to be provided till site, predefined from ERNET.
- viii. Any shifting of site will be done by Contractor, if required.
- ix. Any other activity which may be mutually decided during the project period.

12.11 Vendor Management Services

Contractor shall coordinate with external System Integrator(s) & Service Providers for upkeep of equipment / Network services to meet the SLA

- i. Shall liaison with respective vendors/OEMs, other Contractors, Bandwidth service providers for repairs/replacement of items and/or update/upgrade/troubleshoot the services.
- ii. To perform this activity, the CONTRACTOR shall maintain equipment/service wise database of the various vendors and service providers with details like contact person, telephone numbers, escalation matrix, response time and resolution time commitments, and equipment expiry date of Maintenance Services/Warranty/Software Assurance/Support etc.
- iii. Log and escalate the calls with respective System Integrator(s) /OEM/service provider within 1 hour from occurrence of incident/ problem. Contractor shall also do repetitive pursuance and coordination with them till the equipment repaired/problem is resolved.
- iv. Liaising with existing System Integrator(s) & Service Providers
- v. Report preparation and sharing of same with stakeholders as per the defined periodicity.
- vi. All other tasks as per the Scope of Work and O&M including any other task deemed necessary to carry out the desired work.

12.12 Change management Services

- i. Tracking the changes in hard / soft configurations, changes to applications, changes to policies, users/applying of upgrades / updates / patches, network (WAN/LAN) etc.
- ii. Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and regular updates w.r.t changes should be documented in knowledge bank.

12.13 Help Desk Support

The Contractor shall provide 24 x 7 help desk support from DC to all authorize Users/User departments using the Datacenter network .

- i. The Contractor shall maintain ITIL Compliant helpdesk tool including configuration/ reconfiguration/ upgrade/update.
- ii. Contractor shall log all calls received through any medium viz. telephone/email/in writing/in person, shall generate a ticket mentioning type of problem, Severity level etc. using helpdesk tool and forward the same to concerned team/person
- iii. The request would be made on help desk by the user by dedicated help line number/Specific email account and Contractor shall get approval from the officer in charge of the DC, DR as designated by the ERNET India. The resolution time for such services would be as per SLA. However, the purchaser/authorized entity may scale up the severity level depending upon the requirements.

The indicative lists of such services but not limited to as under –

- a) Change Request for opening/closing of a Port on device
- b) Request for Internet Access as per policy
- c) Change request for Routing Policies

- d) Change Request for Firewall Policy
- e) Request for Installation/Re-Installation of Servers (Hardware only)
- f) Daily/Weekly report generation
- g) SLA report
- h) Any other activity which may be decided during the project period

12.14 Dash boarding and Reporting

SI shall submit the reports on a regular basis in an approved format by ERNET India/CERT-In. The following is only an indicative list of MIS reports that shall be submitted by Contractor to ERNET India/CERT-In and any designated agency by ERNET India/CERT-In. Any other report required in any desired format by ERNET India/CERT-In, the Contractor shall be responsible to share the same as per the frequency desired.

Daily Reports

- 1) Summary of issues / complaints logged at the Help Desk
- 2) Summary of resolved, unresolved and escalated issues / complaints
- 3) Reports for the alarms / incidents reported
- 4) Reports for the alarms / incidents reported
- 5) Log of backups undertaken
- 6) Application monitoring report which will cover underlying infrastructure, application middle ware, Operating System and licenses along with their utilization through an online dashboard

Weekly reports

- 1) Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
- 2) Summary of systems rebooted/VPNs configured / Links.
- 3) Summary of issues / complaints logged with the OEMs.
- 4) Reports for the alarms / incidents reported
- 5) Inventory of spare parts in the DC, DR & remote sites.
- 6) Summary of changes undertaken in the DC, DR & remote sites including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
- 7) Reports of inventory with serial numbers and other unique parameters within
- 8) Any downtime planned in next 4 weeks.

Monthly reports

- 1) Component wise IT & Non IT infrastructure availability and resource utilization.
- 2) Consolidated SLA / (non)- conformance report.
- 3) Summary of component wise DC, DR & remote sites uptime.
- 4) Summary of changes in the DC, DR & remote sites.
- 5) Logs of preventive / scheduled maintenance undertaken.
- 6) Logs of break-fix maintenance undertaken.
- 7) Reports for the alarms / incidents reported
- 8) SLA calculations, Inventory and Assets, Availability of Manpower.
- 9) Open / Closed / In Progress Helpdesk tickets, Feedback, Root causes of regular alarms/problems, Improvement areas.

- 10) Contractor shall undertake proactive monitoring of the entire basic infrastructure and diagnose problems that could arise as part of any component installed in DC, DR and remote locations. The Contractor shall maintain a log of all such diagnosis and notify ERNET India/ CERT-In on a monthly basis in the form of a report.
- 11) Report Software licenses usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the DC, DR & remote sites through an online dashboard.
- 12) VAPT compliance reports if any, updates/upgrades
- 13) Other reports planned and discussed during the course of project.

Quarterly reports

- 1) Consolidated component-wise physical and IT infrastructure availability and resource utilization.
- 2) Summary of all monthly reports
- 3) Quarterly Consolidated SLA reports as per the required templates.
- 4) Any other request on reporting template / parameters as per feedback from ERNET India /Cert-In

Half-Yearly reports

- 1) DC, DR & remote sites Security Audit Report.
- 2) IT infrastructure Upgrade / Obsolescence Report.

Incident Reporting

- 1) Detection of security vulnerability with the available solutions / workarounds for fixing.
- 2) Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.
- 3) Software license violations.

Please note:

- MIS and SLA reports shall be provided by Contractor via automated tool in dashboard. The above given reports are indicative, the Contractor may have to provide additional reports as per the requirement of ERNET India/CERT-In.

13. Manpower for Operation & Management at DC , DR and at Delhi

The Contractor will provide different categories of required nos. of manpower at DC & DR as per the details provided in tender document to provide Operation & day to day maintenance services and to meet the desired SLAs during entire contract period. The domain & qualification wise list of minimum Manpower to be deployed under the project is given below table. However, Contractor may deploy additional manpower to meet the desired SLA at no extra cost during entire contract period. Manpower location may also be shifted between DC and DR as per project requirement. Contractor shall ensure the following before assigning Manpower under this project:

- 1) Contractor must ensure that all the manpower deployed for Operation & maintenance should be on Contractor's or OEM payroll.
- 2) Contractor must follow Labour Laws laid by Government of India.
- 3) The manpower deployed by the Contractor shall not install/use any other unauthorized software etc. (except pre-installed licensed software) and shall not misuse the IT systems of ERNET India/CERT-In.
- 4) At times, in case of exigencies of work, the manpower may be required to work beyond office hours, for which no additional payment will be made by ERNET India to the Contractor .
- 5) If the ERNET India notices that the manpower deployed by Contractor has/have been negligent and careless in rendering the said services, the same shall be communicated immediately to the Contractor. The Contractor will take corrective action immediately, to avoid recurrence of such incidents, which may include providing proper substitutes;
- 6) If any, manpower deployed by the Contractor indulges in theft, misconduct or any illegal/irregular activities, the Contractor/appropriate stakeholders will initiate appropriate action against such manpower besides providing suitable substitutes in its place.
- 7) Contractor has to comply with local labour laws (minimum wages) as well as labour laws of government of India/ State Government.
- 8) The Contractor shall employ only such persons as are qualified and skilled for carrying out the assigned jobs as detailed in Manpower requirement.
- 9) The Contractor shall be responsible for the proper behaviour of the manpower deployed and shall exercise proper control over them, and to ensure that their activities shall not in any way be detrimental to ERNET India. The Contractor shall have to withdraw such manpower with immediate effect, if so desired by ERNET India/ CERT-In.
- 10) The Contractor shall issue Identity Cards on its own name to its manpower deployed for rendering the said services, which at ERNET India's option, would be subject to verification at any time. The ERNET India may refuse the entry into its premises to any manpower of the Contractor not bearing such identity card.
- 11) It is understood between the parties hereto that the Contractor alone shall have the right to take disciplinary action against any manpower engaged/ deployed by it, while no right shall vest in any such manpower to raise any dispute and/or claim whatsoever against ERNET India. ERNET India shall under no circumstances be deemed or treated as the Employer in respect of manpower engaged/deployed by the Contractor for any purpose, whatsoever, nor would ERNET India be liable for any claim(s) whatsoever, of any such manpower.
- 12) Contractor will indemnify ERNET India in case of issues related to manpower deployed at user location.

The deployed resources shall be required to operate from the Data center mentioned in the Bid. The schedule of the sitting arrangement shall be finalized in consultation with ERNET India. The

shift schedule and sitting arrangement may be changed as per the requirement during entire contract period by the User.

13.1 Minimum Manpower to be deployed for one year from the start of Operation and maintenance

Manpower Requirement: The minimum requirement of manpower resources, their qualification and responsibility of each resource is given below. The Contractor has to ensure that appropriate qualified manpower with requisite skill sets is deputed for the project.

The Contractor shall depute the resources as per the requirements for carrying out the O&M Activity and maintaining the SLA. This is minimum indicative list of resources and based on actual requirements, the Contractor may deploy extra manpower to meet the SLA. The ERNET India/CERT-In shall not pay any cost for additional resources required to operate, maintain, monitor & manage the project as per the SLA.

In case deputed employee/staff is not available or is on leave, the Contractor is required to provide the alternative personnel with same or higher technical capabilities of the non-available personnel.

At Data Center (DC) :-

SN	Role	09:30-17:30 hrs	06:00 – 14:00 hrs	14:00 – 22:00 hrs	22:00 – 06:00 hrs	Total
1	Project Manager-	1				1
2	Security Specialist		1	1	1	3
3	Network Specialist		1	1	0	2
4	Network Engineer		1	1	1	3
5	System (Server) Specialist		1	1	1	3
6	System (Server) Engineer		1	1	1	3
7	NMS & DCIM Engineer		1	1	1	3
8	Help Desk Support Staff		1	1	0	2
Total						20

At Disaster Recovery Data Centre (DR):-

SN	Role	09:30-17:30 hrs	06:00 – 14:00 hrs	14:00 – 22:00 hrs	22:00 – 06:00 hrs	Total
1	Security Specialist	1				1
2	Network Specialist		1	1	0	2
3	Network Engineer		1	1	1	3
3	System Specialist		1	1	1	3
4	System (Server) Engineer		1	1	1	3
5	NMS & DCIM Engineer	1				1
8	Help Desk Support Staff	1				1
Total						14

At Shastri Park, Delhi (ERNET/CERT-In premises):-

Sl.No	Manpower Role	Timing (09:00 -18:00)
1	Network Specialist	1
2	NMS/ Help Desk Support	1

Note: O&M for remote Sites will be done by Contractor through its Manpower stationed at their offices. If physical presence is required at remote site for the purpose of O&M then authorise manpower may be sent to the site with an intimation to ERNET India.

13.2 Manpower Specification

Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi

Sl.No	Role	Min. Qualification, Relevant Experience & Certifications
1	Project Manager	B.E./B.Tech/MCA 8 Years relevant experience in IT/ITeS (minimum 6 years' experience for managing large data centers) + CCNP-DC/ JNCIA-DC or equivalent Certified
2	Security Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience in IT Network Management + Certification: OEM certified engineer on proposed security equipment Such as JNCIP-SEC, Fortigate NSE 4, CCNP Security or equivalent

3	Network Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience in IT Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 5 years of work experience on leaf and spine architecture
4	Network Engineer	B.E./B.Tech/MCA in Computer/IT / Electronics + 4 Years relevant experience in Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 3 years of work experience on leaf and spine architecture
5	System (Server) Specialist	B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience of different flavors of OS with Storage + Must have 5 year of experience on offered OEM Servers.
6	System (Server) Engineer	B.E./B.Tech/MCA in Computer/IT / Electronics + 5 Years relevant experience of different flavors of OS with Storage + Must have 3 year of experience on offered OEM Servers.
7	EMS & DCIM Engineer	B.E./B.Tech/MCA + 3 Years relevant experience + Proposed EMS certified engineer, if any or Should have CCNA/JNCIA or equivalent certification.
8	Help Desk Support Staff	B.E./B.Tech/ MCA in Computer/IT / Electronics with 3 Year relevant experience.

13.3 Work profile of Manpower to be deployed

Project Manager

- Should be responsible for data center (DC) and DR activities like installations, hosting, upgradations, migration, incident management, change management, performance tuning activities and patching etc.
- Should be responsible for the project management throughout the entire project lifecycle, including project initiation, project delivery, stakeholder management, post implementation review and project close out / handover.
- Should have to work closely with other team members and Shall be responsible for overall work assigned to Contractor for all the data centres and DR
- Should be responsible to implement International Best Practices in relevant area of data centre like Security, DR Implementation etc.
- Should be responsible for delivery of all project deliverables as per bid
- Should provide technical solutions and strategic recommendations to enhance services quality
- Shift Management
- Vendor Management
- Should communicate technical ideas to technical and non-technical stakeholders is critical. Additionally, the ability to document support procedures to ensure that deployed systems are properly maintained and supported.

Security Specialist

- Should be SPOC for all network security activities at data centre and DR like installations, upgradations, migration, incident, performance tuning activities, reporting and patching etc.
- Design, configure, implement and maintain all security platforms and their associated software, such as routers, switches, firewalls, intrusion detection/intrusion prevention etc.
- Design, review and ongoing assessment of firewall, intrusion detection/intrusion prevention, VPN and other network & security component policies.
- Ensure network security best practices are implemented through auditing: router, switch, firewall configurations, change control, and monitoring.
- Coordinate and extend support for Network/Security services offerings in consultation with ERNET India to ensure customer policy and security requirements are met.
- Responding to security breaches or other security incidents and coordinate with respective OEMs. In case of a new threat is observed to ensure that workaround / patch is made available for the same.
- Responsible for periodically reviewing and validating user access rights and privileges.
- Act as a key liaison between departments and other stakeholders.

Network Specialist & Network Engineer

- Should be responsible for all network activities at data centre and DR like installations, upgradations, migration, incident, performance tuning activities, reporting and patching etc.
- Should be well versed in Switching, Routing and network equipment.
- Should have worked on Leaf & Spine Architecture in Data Center
- Should have good knowledge in monitoring network with tools (Cisco IOS, Junos, PRTG, Netflow, etc.)
- Should have worked on large scale data Center network.
- Management of Configuration changes of switches/routers when required & periodic backup of configurations
- Should be able to configure and troubleshooting of Layer2 protocols, such as: VLAN, Private VLANs, VTP, STP, DTP, Trunking, Stacking, Ethernet channel, DOT1Q, ISL, SVI etc.
- Should be able to configure IPSEC tunnel between locations.
- Should be able to configure and troubleshooting of Layer3 Protocols such as: BGP, EIGRP, OSPF, Static Routing, High Availability Protocols (HSRP, VRRP, GLBP), Floating Static Routing, Failover etc.
- Should provide support for IPv4, IPv6, NTP, ACLs, Route-map, Prefix-Lists, PBR, AAA, TACAS, RADIUS, CEF, IPv6 CEF, SLA, TRACK, SNMP, EEM, Syslog, Flow-export, RADIO, EVPN-VXLAN.
- Should be able to configure and troubleshooting of Network Load Balancers Datacentre core switching and routing upgrade & maintenance.
- Router access control management.
- Fault management of routers and switches.
- Corrective actions to resolve faults to ensure high network uptime.
- Troubleshooting and debugging of problems.
- Deploy monitoring tools for identifying problem areas and early rectifications if require.
- Periodic fine-tuning to ensure optimal network availability

- Regular checking for proper functioning of network and assets deployed
- Should be well versed with EMS tools.
- Incident, Change and Configuration Management, IOS Upgradation, change request management.
- Network Specialist at DC will also look into network issues of DR in liaison with his DR team member.

System Specialist & System Engineer

- Should be responsible for all the server activities at data center and DR like installations, performance tuning activities, reporting etc.
- Should work in 24*7 rotational shifts
- Responsible for all server tickets & alert (for Server HW alerts) response/resolution time management
- Manage OEM / Vender ticket for all servers
- Prepares and maintains weekly and monthly server reports
- To ensure that servers, processes and methodologies as specified are followed to sure effective monitoring, control and support of IT Service delivery
- Make escalation to upper level related to all servers
- SLA Management for all OEM/ Vendors
- Server Specialist at DC will also look into server issues of DR in liaison with his DR team member.

EMS/DCIM Engineer

- Responsible for overall establishment, installation and maintenance of EMS/DCIM solution in Data centres and DR
- Provide data, reporting and trends to IT department and others in ad-hoc, weekly, monthly and as needed
- Co-ordinate with internal teams and handle escalations to ensure issues are resolved quickly with least customer downtime.
- Ensuring continuous monitoring and prompt reporting of / from all assets, service(s).
- Managing the help desk team and evaluate performance
- Responsible for installation and management of EMS solution in Data centre
- Addition and deletion of Datacentre assets in EMS tool
- Incorporation of third party MIBs (such as packet brokers) into EMS.
- Develop daily, weekly and monthly reports of EMS tools as per requirement
- Maintain and develop own knowledge and skills to assist with first time fault resolution
- Development of Knowledge base system.

Help Desk Support Staff

- log all calls received through any medium viz. telephone/email/in writing/in person, shall generate a ticket mentioning type of problem, Severity level etc. using helpdesk tool and forward the same to concerned team/person, Project incharge and user.
 - Correctly logging incidents and faults, categorizing and prioritizing them in line with team procedures
 - Maintain and develop own knowledge and skills to assist with first time fault resolution
 - Sharing knowledge with team colleagues
- Provide customer feedback to the appropriate internal teams

14. Project Handover Plan

The Contractor shall provide the ERNET India/CERT-In or its nominated Contractor with a recommended Handover plan ("HO Plan") which shall deal with at least the following aspects of Handover:

- i. A detailed program of the transfer process that could be used in conjunction with a Replacement Contractor (if any) 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;
- ii. Plans for provision of contingent support to ERNET India/ CERT-In, and New Contractor (if any) for a reasonable period after transfer.
- iii. The SI shall ensure that no downtime of services is attributed due to handover activities. The handover should include but not limited to:
 - a) Process, Policies, Passwords & Guidelines
 - b) Inventory & Assets details (IT, Non-IT and Utilities)
 - c) Operations, Maintenance and Management of responsibilities
 - d) Data Privacy & Security responsibilities
- iv. Contractor must ensure to prepare the detailed handover plan and submit along with the Milestone-1. The handover plan will be reviewed by ERNET India / Cert-In and shall be mutually agreed with Contractor, to be termed as accepted. The handover plan must consider the documentation of following aspects (the below is just an indicative list):
 - a) Standard Operating Procedures for various planned processes and operations
 - b) Current Operating policies, Incident Management
 - c) Physical security controls.
 - d) Schedule and scope of various audits
 - e) Low Level Design Document and High Level Design documentation with network topology
 - f) Acceptance Test Plan
 - g) Asset and Inventory Checklist for DC, DR and Remote Location
 - h) Best Practices followed
 - i) Help desk reports
 - j) Knowledge transfer, Asset Transfer, operations transfer during exit
 - k) Any other activity required to execute systematic handover.
- v. The Contractor shall update the Handover Plan regularly in consultation with ERNET India thereafter to ensure that it is kept relevant and up to date.
- vi. In the event of termination or expiry of contract, each Party shall comply with the Handover Plan.
- vii. Handover plan will be initiated a quarter before the expiry of contract.
- viii. ERNET India/CERT-In at its discretion may extend the transition period if deemed necessary.

Section VIII: Service Level Agreement during Operation & Maintenance

1 Service Level during Operation & Maintenance period for Equipment:

A. For Equipment at DC & DR procured via this bid:

- 1) Contractor has to provide uptime of each equipment and its related services @99.9% for the equipment(s) installed at DC & DR including Phase-1 equipment(s). The uptime shall be calculated on monthly periodicity.
- 2) For the equipment supplied via this bid, a penalty @ 0.5 % of the equipment(s) cost of affected portion* per day or part thereof for first 24 hours, will be deducted for downtime beyond permissible limit. In case, DCIM, EMS, etc. goes non-functional, a penalty @0.5% per day or part thereof for first 24 hours for respective component will be applicable.
- 3) In case fault persists for more than 24 hours then penalty @1.0 % of equipment cost of the affected portion* per day or part thereof will be deducted for downtime beyond permissible limit.
- 4) Penalty of Rs.1000 on per day basis will be charged for equipment(s) whose individual line item price could not be derived from the price bid besides the penalty arising out the affected portion* per day.
- 5) Bidder may keep spare equipment/ parts etc. to keep the services running and minimize the fault duration & penalties.
- 6) No penalty will be imposed for downtime asked by the bidder for preventive maintenance, schedule maintenance, patch upgradation etc. However, any of these activity shall be done only in off peak hours and with due permission from ERNET India/CERT-In.
- 7) In case, SLA breach happens due to the technical dependency on the ERNET India/CERT-In, the penalties would not be applicable on Contractor.
- 8) During O&M, bidder must do preventive maintenance (PM) in every quarter for DC & DR. If PM is missed as per defined frequency, the same should be carried out within next two weeks. Else penalty of Rs. 1,00,000/- per day or part thereof per data centre(DC/DR) for delays will be deducted.

B. For Equipment procured at DC via the Phase-1 bid(by CDAC):

- 1) For the services down due to issues other than hardware fault i.e due to Operations and maintenance activities on Phase-I equipment (i.e. equipment installed via CDAC's bid#) at DC, Penalty @ 1 % of quarterly payment of OPEX per day or part thereof will be deducted for downtime beyond permissible limit.

C. For equipment at remote sites:

- 1) Contractor has to provide monthly uptime of equipment(s) and its related services @99% for the equipment(s) installed at remote sites.
- 2) Penalty @0.25 % of equipment cost of affected portion* per day or part thereof will be deducted for downtime beyond permissible limit.
- 3) In case fault pertains more than 24 hours, Penalty @0.5 % of equipment cost of the affected portion* per day or part thereof will be deducted for downtime beyond permissible limit.
- 4) Contractor may keep spare units, parts to keep the services running and minimize the fault duration & penalties.

- 5) No penalty will be imposed for downtime asked by the bidder for preventive maintenance, schedule maintenance, patch upgradation etc. However, any of these activity shall be done only in off peak hours and due permission from ERNET India.
- 6) In case, SLA breach happens due to the dependency on the ERNET India/CERT-In, the penalties would not be applicable on Contractor.
- 7) During O&M, bidder must do preventive maintenance at least once every year . Payment for last quarter of the O&M shall be released subject to submission of documentary evidence for carrying out of successful PM.

***Affected portion means:** - If any equipment/hardware(s)[e.g. A] is faulty/not functional and other equipment/hardware(s)[e.g. B] which could not function / could not be used due to failure of equipment/hardware(s)[e.g. A], then the affected portion will be equipment/hardware(s)[A]+[B]. For e.g. If both leaf switches are faulty/not functional, due to which the complete server rack is faulty/not functional, then penalty will be imposed on all equipment falling in that particular rack. Similar, penalty calculation w.r.t affected portions will be followed for all types of equipment installed in this project including cabling /intelligent cabling.

D. Help Desk support during O&M period for services:

Onsite Technical team will coordinate ERNET INDIA/CERT-In technical team for the resolution of all IT infrastructure related issues / problems. Support desk shall undertake the following activities:

- i. Log issues / complaints related to IT infrastructure at the Data Centre & Remote Sites and issue an unique ID number against the issue/complaint.
- ii. Assign severity level to each issue / complaint so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels. Category of Service level will be defined and finalised with successful bidder.
- iii. Track each issue/complaint to resolution.
- iv. Escalate the issues/complaints, to ERNET India officials if necessary as per the escalation matrix defined in discussion with ERNET India.
- v. Analyze the issue/complaint statistics and SLA.
- vi. Should provision for all necessary channels for reporting issues to onsite technical team. The incident reporting channels will be the following:
 - Email
 - SMS
 - Web Based
 - Should implement a call logging system in line with the severity levels as mentioned in the SLA.

E. Help Desk Support Services Level

Response time: is defined as the time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and a support team member begins working on the incidence.

Resolution time: is defined as the total time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and the incidence been resolved.

Service Window:

Working Hours: 24x7 (Monday to Sunday)

Priority Level	Response Time	Resolution time *
High	30 minutes#	Within 2 Hours
Low	60 Minutes\$	Within 4 hours

*Resolution Time- In case of Equipment fault then penalty will be governed through Service level of Equipment uptime as mentioned in 1.1 & 1.2 of section VIII.

All configuration issues pertaining to Computing & Networking Equipment and Firewall Management will fall in Priority Level High.

\$Other Issues will be treated as Priority Level Low.

S/N	Definition	Measurement Interval	Penalty
1	“Resolution Time” , means time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk till the time the problem has been fixed and updated as resolved in the helpdesk.	Quarterly	0.1% of quarterly OPEX* value for every one hour delay (on incremental basis) beyond permissible time for High Priority level 0.05% of quarterly OPEX value for every one hour delay (on incremental basis) beyond permissible time for Low Priority level
2	SLA Document submission	Monthly (on 5 th day of every Month)	0.025% of quarterly OPEX value for per day or part thereof delay (on incremental basis) beyond permissible time
3.	Non Provisioning of Any required document / artifact such as reports etc.	Monthly (on 5 th day of every Month)	Rs.1000 per day delay in submission of desired document / artifact.

Note:- The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value. In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2 of Section-III

F. Security and Incident Management Service Levels

(There will not be any penalty capping for this section)

S/N	Definition	Measurement Interval	Target	Penalty
1	For every Virus attack reported and not resolved within 36 hrs from the time of attack	Quarterly	36 hours	Rs. 50,000 for delay of every 24 hours or its part. If more than three virus attacks are reported in a quarter, then Rs. 1,00,000/- per incident would be deducted as penalty.
	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Every instance in the Quarter	At every instance	Rs.5,00,000 per instance.
	For every Intrusion reported by firewall and not resolved within 2 hour from the time of report.	Every instance in the Quarter	Beyond 2 hrs	Rs. 50,000
	Patch Management (including rules updation in Firewalls)	Every instance in the Quarter	Within 2 hrs time from the approved request	No Penalty
> 3hrs and <=4hrs			Rs.50,000	
Beyond 5hrs for every 3 hrs			Rs.1,00,000	

G. Manpower Service Level Agreement:

SLA would be applicable from the Milestone-1 and in operations and maintenance phase of the project. SLA would be applicable on the availability of manpower and the service levels mentioned below:

S. No.	Service level agreement	Penalties for non-compliance
1	Non-deployment of total manpower mentioned in the contract as per the date of joining	Operation and Maintenance billing will be started only after deployment of total Manpower as per contract. Further 0.5% of quarterly OPEX value per day will be deducted from due payments/ performance security for non-deployment of complete manpower.
2	If the employee is found responsible for any theft, loss of material/ articles and damages	Immediate payment in actuals, equivalent to the value of the article theft/lost/damaged. Replacement within 3 day/cancellation of contract as decided by the ERNET India depending on the gravity of the act.
3	If the employee is found responsible for disobedience/ misconduct	Warning/counselling/Immediate replacement of resource within 3 days as decided by ERNET India depending on the gravity of the act
4	If the employee is absent for more than 3 days without informing or taking prior approval	0.5% of quarterly OPEX value for per day per manpower.
5	If employee is on leave	Contractor shall arrange replacement of manpower during the leave of employee. 0.5% of quarterly OPEX value for per day per manpower, if no manpower arranged during the leave period of employee.
6	If the employee is found responsible for adopting illegal and foul methods or exercising any corrupt practice in collusion with any third party or officials at the workplace	Immediate replacement within 3 days/ cancellation of the contract with cancellation charges @ 5% of the contract value or as decided by ERNET India depending on the gravity of the act
7	Up to 4 replacements	No penalty
8	More than 4	Rs. 10,000/-per replacement (applicable beyond 4 replacements). No penalty will be imposed if Manpower resign from Contractor organisation or if requested by ERNET India/CERT-In for replacement of manpower due to incompetency.

BIDDING FORMS

Form 1: Bid Form (Covering Letter)

(To be submitted as part of Technical bid, along with supporting documents) (On Bidder's Letter-head)

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park, Delhi-110053

Ref: Your Tender Document No. Tend No./ xxxx;

Sir/ Madam

Having examined the abovementioned Tender Document, we, the undersigned, hereby upload our Technical and Financial bid (Price Schedule) for the supply of Equipment(s) and Services in conformity with the said Tender Documents.

1) **Our Credentials:**

We are submitting this bid on our behalf, registered in India under the Indian Companies Act 1956/2013 as amended. Our company law and taxation regulatory requirements and authorization for signatories and related documents are submitted in Form 1.1 (Bidder Information).

2) **Our Eligibility and Qualifications to participate**

We comply with all the eligibility criteria stipulated in this Tender Document, and the relevant declarations are made along with documents in Form 1.2 of this bid-form. We fully meet the qualification criteria stipulated in this Tender Document, and the relevant details are submitted along with documents in Form 4: 'Qualification Criteria - Compliance & Form 4.1- Experience Statement.

3) **Our Bid to supply of Equipment & Services:**

We offer to supply the subject Equipment(s) of requisite quality and within Delivery Schedules in conformity with the Tender Document. The relevant details are submitted in Form 2: 'Bill of Material - Compliance and Form 3: 'Technical Specifications - Compliance.'

4) **Prices:**

We hereby offer to perform the Services at our lowest prices. The prices in this offer have been arrived at independently, without restricting competition, any consultation, communication, or agreement with any other bidder or competitor relating to:

- i) those prices; or
- ii) the intention to submit an offer; or
- iii) the methods or factors used to calculate the prices offered.

The prices in this offer have neither been nor shall be knowingly disclosed by us, directly or indirectly, to any other bidder or competitor before bid opening or contract award unless otherwise required by law.

5) **Affirmation to terms and conditions of the Tender Document:**

We have understood the complete terms and conditions of the Tender Document. We accept and comply with these terms and conditions without reservations and deviations.

6) Bid Securing Declaration

We have submitted the Bid Securing Declaration in stipulated format vide Form 7: 'Documents Relating to bid security.'

7) Abiding by the Bid Validity

We agree to keep our bid valid for acceptance for a period upto 75 days, as required in the Tender Document or for a subsequently extended period, if any, agreed to by us and are aware of penalties in this regard stipulated in the Tender Document in case we fail to do so.

8) Non-tempering of Downloaded Tender Document and Uploaded Scanned Copies

We confirm that we have not changed/ edited the contents of the downloaded Tender Document. We realise that any such change noticed at any stage, including after the contract award, shall be liable to punitive action in this regard stipulated in the Tender Document. We also confirm that scanned copies of documents/ affidavits/ undertakings uploaded along with our Technical bid are valid, true, and correct to the best of our knowledge and belief. If any dispute arises related to the validity and truthfulness of such documents/ affidavits/ undertakings, we shall be responsible for the same. Upon accepting our Financial bid, we undertake to submit for scrutiny, on-demand by the ERNET India, originals, and self-certified copies of all such certificates, documents, affidavits/ undertakings.

9) A Binding Contract:

We further confirm that, if our bid is accepted, all such terms and conditions shall continue to be acceptable and applicable to the resultant contract as defined in tender document.

10) Performance Guarantee and Signing the contract

We further confirm that, if our bid is accepted, we shall provide you with performance security of the required amount stipulated in the Tender Document for the due performance of the contract. We are fully aware that in the event of our failure to deposit the required security amount, the ERNET India has the right to avail any or all punitive actions laid down in this regard, stipulated in the Tender Document.

11) Signatories:

We confirm that we are duly authorized to submit this bid and make commitments on behalf of the Bidder. Supporting documents are submitted in Form 1.1 annexed herewith. We acknowledge that our digital/digitized signature is valid and legally binding.

12) Rights of the ERNET India to Reject bid(s):

We further understand that you are not bound to accept the lowest or any bid you may receive against your above-referred Tender Document.

.....
(Signature with date)

.....
(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 1.1: Bidder Information

(To be submitted as part of Technical bid) (On Company Letter-head)

(Along with supporting documents, if any)

Bidder's Name _____

[Address and Contact Details]

Date.....

Tender Document No. Tend No./ xxxx;

Note: Bidder shall fill in this Form following the instructions indicated below. No alterations to its format shall be permitted, and no substitutions shall be accepted. Bidder shall enclose certified copies of the documentary proof/ evidence to substantiate the corresponding statement wherever necessary and applicable. Bidder's wrong or misleading information then ERNET India may invoke Bid Security Declaration .

(Please tick appropriate boxes or strike out sentences/ phrases not applicable to you)

1) Bidder/ Contractor particulars:

- (a) Name of the Company:.....
- (b) Corporate Identity No. (CIN):
- (c) GeM Supplier ID
- (d) Place of Registration
- (e) Complete Postal Address:
- (f) Pin code:
- (g) Telephone nos.:
- (h) Mobile Nos.:
- (i) Contact persons/ Designation:
- (j) Email IDs:

Submit documents to demonstrate eligibility as per NIT-Clause 3- Certificate of incorporation/Registration attested by Company Secretary/ Authorized Signatory.

2) Taxation Registrations:

- (a) PAN number:
- (b) GSTIN number:

We solemnly declare that our GST rating on the GST portal/ Govt. official website is not negative/ blacklisted.

Documents to be submitted: Self-attested Copies of PAN card and GSTIN Registration.

3) Authorization of Person(s) signing the bid on behalf of the Bidder

- (a) Full Name: _____
- (b) Designation: _____
- (c) Signing as:

A company. The person signing the bid is the constituted attorney by a resolution passed by the Board of Directors or Power of attorney given on stamp paper by authroise person.

Documents to be submitted: Power of Attorney/ Board Resolution

4) Bidder's Authorized Representative Information

- (a) Name:
- (b) Address:
- (c) Telephone/ Mobile numbers:
- (d) Email Address:

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 1.2: Eligibility Declarations

(To be submitted as part of Technical bid)

(On Company Letter-head)

(Along with supporting documents, if any)

Tender Document No. Tend No./ xxxx;

Bidder's Name _____

[Address and Contact Details]

Date.....

Note: The list below is indicative only. You may attach more documents as required to confirm your eligibility criteria.

Eligibility Declarations

(Please tick appropriate boxes or cross out any declaration not applicable to the Bidder)

We hereby confirm that we are comply with all the stipulation of NIT-clause 3 and ITB-clause 3.2 and declare as under and shall provide evidence of our continued eligibility to the ERNET India as may be requested:

- 1) **Legal Entity of Bidder:** _____
- 2) We solemnly declare that we :
 - a. are not be insolvent, in receivership, bankrupt or being wound up and not have its business activities suspended by Government.
 - b. Are not stand declared ineligible/ blacklisted/ banned/ debarred by Government .
- 3) The prices quoted should be competitive and without adopting any unfair/ unethical/ anti-competitive means. No attempt should be made to induce any other bidder to submit or not to submit an offer for restricting competition.
- 4) We certify that we fulfil any other additional eligibility condition if prescribed in Tender Document.
- 5) We have gone through F.No.6/18/2019 – PPD dated 23rd July 2020 issued by Department of Public Procurement, Ministry of Finance, Govt. of India and certify as follows:

I hereby certify that the <<<<bidder's name>>>> :

(i) is not from such a country

or

(ii) is from such a country and has been registered with the Competent Authority in India which makes the bidder eligible to participate in this Tender. [Evidence of valid registration by the Competent Authority attached.]

I hereby certify that <<<<<bidder name>>> fulfils all requirements in this regard and is eligible to be considered.

{Strike out inapplicable clause i.e. clause (i) or (ii)}

6) Make in India Status:

Having read and understood the Public Procurement (Preference to Make in India PPP - MII) Order, 2017 (as amended and revised till date) and related notifications from the relevant Nodal Ministry/ Department, and solemnly declare the following:

a) Self-Certification for the category of suppliers:

(Provide a certificate from statutory auditors/ cost accountant for Class-I or Class-II Local Suppliers). Details of local content and location(s) at which value addition is made are as follows:

Local Content and %age	
Location(s) of value addition	

Therefore, we certify that we qualify for the following category of the supplier (tick the appropriate category):

- Class-I Local Supplier/
- Class-II Local Supplier/
- Non-Local Supplier.

b) We also declare that.

- There is no country whose bidders have been notified as ineligible on a reciprocal basis under this order for the offered Services, or
- We do not belong to any Country whose bidders are notified as ineligible on a reciprocal basis under this order for the offered Services.

7) Penalties for false or misleading declarations:

We hereby confirm that the particulars given above are factually correct and nothing is concealed and undertake to advise any future changes to the above details. We understand that that ERNET India may invoke Bid Security Declaration, if any wrong or misleading self-declaration submitted by us.

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 2: Bill of Material - Compliance

(on Company Official Letter Head)

Bidder's Name _____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park, Delhi-110053

Ref: Tender Document No. Tender No./ xxxx;

Subject: Bill of Material (BoM) Compliance

There are no deviations (null deviations) in Bill of Material mention in Section IV in Tender Document. <<M/s Bidder's Name ->> certify that our proposal includes all the equipment & services specified in tender document.

We understand that the requirement of equipment(s) & services briefed in **Section-IV-Bill of Material**; we confirm that we have undertaken our own assessment for complete implementation of project and accordingly we have considered extra Equipment, software, application and services etc. (if any) will be provided by << M/s Bidder's Name >>>> to complete the project.

This is to certify that our proposed bid included all the Equipment(s) and service mentioned in **Section-IV-Bill of Material** as well as other material or service based on self-assessment to complete the project and meets all the requirements of the tender document including but not limited to Scope of Work (including SLAs), Business Requirements and Functional Specifications/ Requirements.

In case, any equipment or software or services is found non-compliant at any stage during project implementation or after acceptance, it would be replaced with a fully compliant product/ solution at no additional cost to ERNET India/ CERT-In. In case of non-adherence of this activity, ERNET India reserves the right to cancel the contract, in case the said Contract is awarded to us by ERNET India.

We shall comply with Warranty requirements in the Tender Document.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work.

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form3: Technical Specifications- Compliance

(on Company Official Letter Head)

Bidder's Name_____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
Shastri Park,Delhi-110053

Ref: Tender Document No. Tender No./ xxxx;

Subject: **Section V- Technical Specification Compliance**

There are no deviations (null deviations) in Technical Specification mention in **Section V- Technical Specification** in Tender Document. <<M/s----->> certify that our proposal fulfil specification of each Equipment & Service specified in tender document.

We understand that the Specification of equipment(s) & services briefed in **Section V- Technical Specification**; we certify that our proposed equipment(s) & services are same or higher than the minimum technical specifications as given in the tender document.

In case, any equipment or software or services is found non-compliant at any stage during project implementation or after acceptance, it would be replaced with a fully compliant product/ solution at no additional cost to ERNET India/ CERT-In. In case of non-adherence of this activity, ERNET India reserves the right to cancel the contract, in case the said Contract is awarded to us by ERNET India.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components, specifications and our obligations, for meeting the scope of work.

Enclosure: -

- 1. Compliance Statement of Section- V and required and relevant documents like technical data, literature, drawings, datasheets, test Reports/ Certificates and or/ or Type Test Certificates (if applicable/ necessary) with supporting documents, to establish that the Equipment and Services offered in the bid fully conform to the Equipment and Services specified by the ERNET India in the Tender Document along with this compliance.**
- 2. Make and Model of offered equipment(s) is attached along with this form as per for form 3 A.**

Yours faithfully,

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form3A: Unpriced Make & Model Details- Compliance

PART A								
Unpriced Make & Model Details- Compliance								
Sl. No.	ITEM	Make	Model	MAF Submitted (Yes/No)	Compliance of Section-V along with Cross reference submitted (Yes/No)	Datasheet submitted (Yes/No)	Provide Datasheet Website URL	Price Quoted in Financial Bid (Yes /No)
1	Server Category-1							
2A	Server Category-2 (4U) with 60 HDD in Each Server							
2B	Server Category-2 (6U) with 84 HDD in Each DAS							
3	Server Category-3							
4	Server Category-4							
5	Server Category-5							
6	Server Category-6							
7	Server Category-7							
8	Server Category-9							
9	Server Category-10							
10	Server Category-11							
11	Server Category-13							
12	Server Category-14							
13	Server Category-16							

14	DC Spine Switch							
15	DC Leaf Switch							
16	DC Core Switch							
17	DC OOB Access Switch							
18	Layer-3 Access Switch							
19	DC CE Router							
20	DC Border Leaf Switch							
21	DC Internet Router							
22	DC Interconnect Switch - Type 1							
23	DC Interconnect Switch - Type 2							
24	DC WAN Switch							
25	SFP-10G-SR4							
26	SFP-10G-LR4							
27	QFSP 28 -SR4							
28	QFSP-28-LR4							
29	Remote Router cum Firewall							
30	Internet Firewall with IPS							
31	DC Internal Firewall							
32	DC Solution Firewall							
33	AAA Appliance							
34	Load balancer							
35	Network Detection & Response (NDR)							
36	IPS&IDS							
37	SSL VPN Gateway							
38	Active Directory Solution							
39	Console management server							
40	KVM Console							
41	Portable KVM console adapter							
42	Monitoring and management tool for servers							

43	Fireproof Vault (200litre)							
44	Degausser							
45	Data Diode							
46	Intelligent Cabling (includes all required accessories briefed in specs for 70 Racks in DC).							
47	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 70 Racks in DC . One Monitor can maximum monitor 2 Racks							
48	Intelligent (AIM) system Software for 10K or 15k Ports in DC as defined in specification							
49	Intelligent Cabling (includes all required accessories briefed in specs for 50 Racks in DR) -Specifications similar to s.n. 46							
50	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 50 Racks in DR . One Monitor can maximum monitor 2 Racks- Specifications similar to s.n. 47							
51	Intelligent (AIM) system Software for 10k Ports in DR-Specifications similar to s.n. 48							
52	Smart Single Rack (usable space 25U)							
53	Non Smart Rack with Redundant IPDU							
54	65 Inch LED Display							
55	Heavy Duty Workstation							
56	Heavy Duty Laptop							
57	Heavy Duty Color Printer							
58	Privileged Access Manager							
59	Any other Item							

Part B

Unpriced Make & Model Details- Compliance

S/N	Item	Make	Model	MAF Submitted (Yes/No)	Compliance of Section-V along with Cross reference submitted (Yes/No)	Datasheet submitted (Yes/No)	Provide Datasheet Website URL	Price Quoted in Financial Bid (Yes /No)
1	Data Center Infrastructure Management (DCIM)							
2	RF Id Based Physical Asset Tracking							
3	Heat Humidity Sensor Solution							
4	RF Id based Physical Asset Tracking Tags							
5	RF Id Rack Identifiers							
6	RF Id Based Heat and Humidity Sensors							
7	Communication Gateways for Communication on RF							
8	Handheld scanner to read barcode / QR codes at DC & DR							
9	Barcode Printer / QR codes with consumables							
10	EMS Solution							
11	IPAM and Switch Port management							

Part C			
Unpriced O&M including Manpower- Compliance			
S/N	Item (Operation and Maintenance for DC, DR and Remote Sites)	Compliance as per Section-V (Yes/No)	Price Quoted in Financial Bid (Yes /No)
	Operation and Maintenance for DC, DR and Remote Sites		
1	Operation and Maintenance (O&M) of DC along with deployment of 20 Technical Manpower at DC		
2	Operation and Maintenance of DR along with deployment of 14 Technical Manpower at DR		
3	Operation and Maintenance of Remote Sites		
4	Deployment of 2 Technical Manpower for Technical Support at Delhi		

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form4: Qualification Criteria - Compliance

(on Company Official Letter Head)

Bidder's Name _____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park, Delhi-110053

Ref: Tender Document No. Tender No./ xxxx;

Subject: **Section-VI- Qualification Criteria - Compliance**

Note to Bidders: Furnish statements and documents to confirm conformity to Qualification Criteria may be mentioned/ attached here. You may attach documents as required for qualification criteria. Add additional details not covered elsewhere in your bid in this regard. Non-submission or incomplete submission of documents may lead to rejection of the bid as nonresponsive.

Documents Attached supporting the compliance to qualification criteria in Section-VI:

Sr	Document Attached, duly filled, signed, and copies self-attested
1	
2	
3	
..	

Yours faithfully,

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form5: Terms & Conditions- Compliance

(on Company Official Letter Head)

Bidder's Name_____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park,Delhi-110053

Ref: Tender Document No. Tender No./ xxxx;

Subject: **Terms & Conditions- Compliance**

- 1) With reference to our Bid submitted against the above referred Tender no....., we hereby confirm that we comply with all terms, conditions and specifications of the Tender Documents read in conjunction with Amendment(s)/Corrigendum(s) / Clarification(s) (if any) issued by ERNET India prior to last date of submission of bids and the same has been taken into consideration while submitting our bid and we declare that we have not taken any deviation in this regard.

- 2) We further confirm that any deviation, variation or additional conditions etc. or any mention, contrary to Bidding Documents and its Amendment(s)/Corrigendum(s) / Clarification(s) (if any) as mentioned at 1.0 above found anywhere in our bid, implicit or explicit, shall stand unconditionally withdrawn, without any cost implication whatsoever to ERNET India.

Yours faithfully,

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 6: Check-List for Bidders

(To be submitted as part of Technical bid)

(on Company Letter-head)

Bidder's Name _____

[Address and Contact Details]

Date.....

Tender Document No. Tend No./ xxxx;

Note to Bidders: This check-list is merely to help the bidders to prepare their bids, it does not override or modify the requirement of the tender. Bidders must do their own due diligence also.

S.No.	Documents submitted, duly filled, signed	Yes/ No/ NA
1.	Form 1. Bid Form (to serve as covering letter and declarations applicable for both the Technical bid and Financial bid)	
2.	Form 1.1: Bidder Information along with following Document in 2.a, 2.b and 2.c	
	2.a) Self-attested copy of Registration certificates etc. of the company.	
	2.b) Self-attested copy of PAN & GSTIN Registration.	
3.	Self-attested copy of Power of Attorney/Board Resolution etc. authorizing signatories on stamp paper to sign the bid.	
4.	Form 1.2: Eligibility Declarations, along with supporting documents in 3.a	
	3.a) Self-attested copy of Registration certificate for bidders from restricted neighbouring countries, if any	
5.	Form 2: Bill of Material – Compliance	
6.	Form 3: Technical Specifications – Compliance of Section-V	
	6.a) Relevant documents - technical data, literature, datasheets, drawings, cross reference to each individual points of the specification and other relevant proposal/bid documents.	
	6.b) Form 3.A: Unpriced Make & Model Details- Compliance	
7.	Form 4: Qualification Criteria – Compliance Documents Attached supporting the compliance to qualification criteria of Bidder and its OEM	
	7.a) Valid ISO 9001:2015, ISO 20000, ISO 27001:2013 Certificates as defined in section -VI {Clause A. (1)}	
	7.b) Annual financial turnover and network as defined in section - VI {Clause A. (3)}	
	7.c) Experience of successful implementation of similar project(s) as defined in section -VI {Clause A. (4)}	
	7.d) Experience of successful implementation as defined in section - VI {Clause A. (5)}	

	7.4e) Experience of successful implementation of Supply & Installation at 100 locations as defined in section –VI {Clause A. (6)}	
	7.f) Undertaking for Own office at following cities as defined in section –VI {Clause A. (7)}	
	7.g) OEM Authorisation Form (MAF) for each product quoted in the bid as defined in section –VI {Clause A. (8)}	
	7.h) Dedicated/Toll free no. for service support as defined in section –VI{Clause A. (9)}	
	7.i) Malicious Code Certificate as defined in section –VI {Clause A. (10)}	
	7.j) OEM <i>Self-certification of TAC availability and Dedicated/Toll free number as per Section-VI Clause B.(1)</i>	
	7.k) Minimum annual average financial for OEM of equipment as defined in Table at <i>Section-VI Clause B.(2)</i>	
	7.l) OEM’s Self Declaration for not debarred/blacklisted/suspended by Government <i>Section-VI Clause B.(3)</i>	
	7.m) Relevant documents of OEM for Product/Software Solution Supply and installation as per <i>as per Section-VI Clause B.(4)</i>	
	7.n) OEM’s Website URL for offered equipment(s) in Form 3.1 <i>as per Section-VI Clause B.(5)</i>	
	7.o) Malicious Code Certification by OEM as defined in section –VI Clause B.(6)	
8.	Form 5: Terms and Condition compliance	
9	Form 6: This Checklist	
10	Form 7: Documents relating to Bid Security	
11	Form 8: Duly signed Integrity Pact	
12	Form 9: Make In India Certificate	
13	Form 10: Non-Disclosure Agreement	
14	Priced Schedule {Financial Bid(BOQ)} as per Tender Document Upload it on GeM at "upload Financial Document" tab on GeM Portal.	
15	Any other requirements, if stipulated in Tender Document or if considered relevant by the Bidder	

Yours faithfully,

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 7: Documents relating to Bid Security.

Note: To be submitted as part of Technical bid, along with supporting documents

Bid Securing Declaration

(on Company Letter-head)

Bidder's Name _____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park, Delhi-110053
Ref: Tender Document No. Tend No./ xxxx;

Sir/ Madam

We, the undersigned, solemnly declare that:

We understand that according to the conditions of this Tender Document, the bid must be supported by a Bid Securing Declaration in lieu of Bid Security.

We unconditionally accept the conditions of this Bid Securing Declaration. We understand that we shall stand automatically suspended from being eligible for bidding in any tender in Procuring Organisation for 2 years from the date of opening of this bid if we breach our obligation(s) under the tender conditions if we:

- 1) withdraw/ amend/ impair/ derogate, in any respect, from our bid, within the bid validity; or
- 2) being notified within the bid validity of the acceptance of our bid by the ERNET India:
refused to or failed to produce the original documents for scrutiny or the required Performance Security within the stipulated time under the conditions of the Tender Document.

We know that this bid-Securing Declaration shall expire if the contract is not awarded to us, upon:

- 1) receipt by us of your notification
 - (a) of cancellation of the entire tender process or rejection of all bids or
 - (b) of the name of the successful bidder or
- 2) forty-five days after the expiration of the bid validity or any extension to it.

Yours faithfully,
(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form8: Integrity Pact

ERNET India hereinafter referred to as "ERNET"

And

-----[bidder (s) participating in this tender] hereinafter referred to as "The Bidder/Contractor"

Preamble

ERNET India invites online bids (e-tender for) for: **"Selection of System Integrator for setting up of ICT Infrastructure at Data Centres and Remote Sites for CERT-In and Operation & Maintenance"**

ERNET India values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, ERNET will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for Compliance with the principles mentioned above.

Section 1- Commitments of ERNET

1. ERNET commits itself to take all measures necessary to prevent corruption and to observe the following principles: -
 - a. No employee of ERNET, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
 - b. ERNET will during the tender process treat all Bidder(s) with equity and reason. ERNET will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder (s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.
 - c. ERNET India will exclude from the process all known prejudiced persons.
2. If ERNET India obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, ERNET India will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) / Contractor(s)

1. The Bidder(s) / Contractor(s) commit himself to take all measures necessary to prevent corruption. The bidder commits himself to observe the following principles during his participation in the tender process and during the contract execution:
 - a. The Bidder(s) / contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of ERNET's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage or during the execution of the contract.
 - b. The Bidder(s) / Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to

- prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
- c. The Bidder(s) / Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) / Contractors will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by ERNET as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
 - d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s) / Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" as annexed and marked as Annexure.
 - e. The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.
2. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from tender process and exclusion from future contracts

- If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, ERNET is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the Government/ERNET India's procedure on banning of the business dealings/bidders/contractors, etc.

Section 4: Compensation for Damages

- a. If ERNET India has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, ERNET is entitled to enforce Bid Security Declaration.
- b. If ERNET India has terminated the contract according to section 3, or if ERNET is entitled to terminated the contract according to section 3, ERNET shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value and/or the amount equivalent to Performance Security or from any due payment to the bidder.

Section 5: Previous Transgression

- a. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any other public sector enterprise in India that could justify his exclusion from the tender process.
- b. If the bidder makes incorrect statement on this subject, he can be disqualified from the tender process for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders/Contractors/Subcontractors

- a. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to ERNET before contract signing.
- b. ERNET India will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.
- c. ERNET India will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation Bidder(s)/ Contractor(s)/Sub contractor(s)

If ERNET India obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if ERNET has substantive suspicion in this regard, ERNET will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor/Monitors

1. ERNET India appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Director General, ERNET.
3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of ERNET including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality.
4. ERNET will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between ERNET and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of ERNET and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The Monitor will submit a written report to the Director General, ERNET within 8 to 10 weeks from the date of reference or intimation to him by ERNET and, should the occasion arise, submit proposals for correcting problematic situations.
7. Monitor shall be entitled to compensation on the same terms as being extended to / provided to Director level in the ERNET India or as decided by Director General of ERNET India.
8. If the Monitor has reported to the Director General ERNET, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Director General ERNET has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
9. The word 'Monitor' would include both singular and plural

Section 9 - Pact Duration

1. This pact begins when both parties have legally signed it. It expires for the Contractor 10 months after the last payment under the contract or after 10 months from the expiry of Rate Contract (RC) whichever be later and for all other Bidders 12 months from the contract has been awarded.
2. If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Director General of ERNET.

Section 10 - Other provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of ERNET, i.e. New Delhi.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. Issues like Warranty/ Guarantee etc., shall be outside the purview of IEMs

(For & on behalf of ERNET India)
(Office Seal)

(For & on behalf of Bidder)
(Office Seal)

Place-----

Date-----

Witness 1: (Name & Address)_____

Witness 2: (Name & Address)_____

Form 9 : Make in India Certificate

Make in India Certificate

(on Company Letter-head)

Bidder's Name _____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
Shastri Park, Delhi-110053

Ref: Tender Document No. Tender No./ xxxx;

In line with Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020 and its amendments, we hereby certify that we M/s _____ are local supplier meeting the requirement of minimum local content i.e., ____% against ERNET India Tender No..... dated..... We qualify as a _____ (Class-I or Class II) local supplier. Detail of locations at which local value addition is/will be made for items as follows:

1. -----
 2. -----
 3. -----
- Etc..

We also certify that we have used mechanism to calculate the local content as per information given by DPIIT at <https://dpiit.gov.in/sites/default/files/RTI%20FAQ.pdf>.

We also understand, false declarations will be in breach of the code of integrity under rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

Annexure: - OEMs Make in India declarations attached.

Yours faithfully,

(Signature with date)

.....

(Name and designation)

Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Form 10: Non-Disclosure Agreement (To be submitted on Non-Judicial Stamp Paper of Rs 100/-)

This Agreement is made as on the _____, between **ERNET India, an autonomous society under the administrative control of Ministry of Electronics and Information Technology, Government of India** called as “**ERNET India**” through its Director General which expression shall unless repugnant to the subject or the context mean and include its successors, nominees or assigns.

and

<<< **Contractor Name**>>> called as “-----” through its ----- which expression shall unless repugnant to the subject or the context mean and include its successors, nominees or assigns.

ERNET India and <<Contractor Name>> are sometimes referred to herein individually as “Party” and collectively as “Parties”.

Tender No. “Selection of System Integrator for setting up of ICT Infrastructure at Data Centers and Remote Sites for CERT-In and Operation & Maintenance” and Contract no..... (hereinafter referred as “Project”). ERNET India and <<Contractor Name>> have entered into a contract to deliver this project, Now, both the parties enter into this agreement and agree that information provided and available with each party

in respect of this project is to be used only for the specific project purpose and parties are required to protect such confidential information from unauthorized use and disclosure.

In consideration of the other party’s disclosure of such information, each party agrees as follows:

1. This Agreement will apply to all confidential and proprietary information disclosed, owned or collected by one party to the other party, including information generated under this project, which the disclosing party identifies in writing or otherwise as confidential to the receiving party (“**Confidential information**”). Information consists of certain specifications, designs, plans, drawings and /or technical information, software, data etc, and all copies and derivatives containing such information, that may be disclosed to one another for and during the purpose, which a party considers proprietary or confidential (“**Information**”). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to one party (hereinafter referred to as the receiving party) by the other party (hereinafter referred to as one disclosing party). Information shall be subject to this Agreement, if it is in tangible form, only if clearly marked as proprietary or confidential as the case may be, when disclosed to the receiving party or, if not in tangible form, its proprietary nature must first be announced, and it must be reduced to writing and furnished to the

receiving party.

2. ERNET India and <<Contractor Name>> hereby agree that during and after the Agreement Period:
 - a) The receiving party shall use Information only for the Purpose, shall hold Information in confidence using the same degree of care as it normally exercises to protect its own proprietary information, but not less than reasonable care, taking into account the nature of the Information, and shall grant access to Information only to its employees who have a need to know, but only to the extent necessary to carry out the business purpose of this project as defined, shall cause its employees, outsourced agencies, vendors, implementation partners and contract employees to comply with the provisions of this Agreement applicable to the receiving party, shall reproduce Information only to the extent essential for fulfilling the purpose, and shall prevent disclosure of information to third parties.
 - b) Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been destroyed.
3. The foregoing restrictions on each party's use or disclosure of Information shall not apply to Information that the receiving party can demonstrate which:-
 - a) was independently developed by or for the receiving party without reference to the Information, or was received without restrictions; or
 - b) has become generally available to the public without breach of confidentiality obligations of the receiving party; or
 - c) was in the receiving party's possession without restriction or was known by the receiving party without restriction in vogue at the time of disclosure; or
 - d) is the subject of a subpoena or other legal or administrative stipulated requirement demand for disclosure; provided, however that the receiving party has given the disclosing party prompt notice of such requirement for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure and appropriate protective order; or
 - e) is disclosed with the prior written consent of the disclosing party; or
 - f) was in its possession or known to it by being in its use or being recorded in its files or computers or other recording media prior to receipt from the disclosing party and was not previously acquired by the receiving party from the disclosing party under an obligation of confidence; or
 - g) the receiving party obtains or has available from a source other than the disclosing party without breach by the receiving party or such source of any obligation of confidentiality or non-use towards the disclosing party.
4. Each party agrees not to remove any of the other party's Confidential Information from the premises and sites of the disclosing party without the disclosing party's prior written approval. Each party agrees to exercise extreme care in protecting the confidentiality of any confidential information which is removed, only with the disclosing party's prior written approval, from the disclosing party's premises and sites. Each party agrees to comply with any and all terms and conditions the disclosing party's may impose upon any such approved removal, such as conditions that the removed confidential information and all copies must be returned by a certain date, and that no copies are to be make

off of the premises.

5. Upon the disclosing party's request, the receiving party will promptly return to the disclosing party all tangible items containing or consisting of the disclosing party's confidential information all copies thereof.
6. Each party recognizes and agrees that all of the disclosing party's confidential information is owned solely by the disclosing party (or its licensors) and that the unauthorized disclosure or use of such confidential information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain. Accordingly, each party agrees that the disclosing party will have the right to obtain an immediate injunction enjoining any breach of this agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity or may seek the intervention of Director General, ERNET India for such a breach.
7. Access to information hereunder shall not preclude an individual who has seen such information for the purpose of this agreement from working on future projects for the receiving party which relate to similar subject matters provided that such individual does not make reference to the information and does not copy the substance of the information during the confidentiality period thereafter as required by applicable law. Furthermore nothing contained herein shall be construed as imposing any restriction on the receiving party's disclosure or use of any general learning, skills or know how developed by the receiving party's personnel under this agreement, if such disclosure and use would be regarded by a person of ordinary skill in the relevant area as not constituting a disclosure or use of the information.
8. As between the parties, all information shall remain the property of the disclosing party. By disclosing information or executing this agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection rights, trade secret or any other intellectual property right. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this agreement and the disclosure of information pursuant to this agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase, or sale or to enter into any additional agreement of any kind.
9. Either party's failure to enforce any provision, right or remedy under this agreement shall not constitute a waiver of such provision, right or remedy.
10. This Agreement will be construed in, interpreted and applied in accordance with the laws of India.
11. That in case of any dispute or differences, breach & violation relating to the terms of this agreement, the said matter or dispute, difference shall be referred to Director General, ERNET India for his decision in this regard. The decision of the Director General, ERNET India will be final and binding on both the parties.
12. This Agreement constitutes the entire agreement of the parties with respect to the parties respective obligations in connection with Information disclosed hereunder and supersedes all prior oral and written agreements and discussions with respect thereto.
13. The parties can amend or modify this agreement only by a writing duly executed by their

respective authorized representatives. Neither party shall assign this Agreement without first securing the other Party's written consent.

14. This Agreement will remain in effect during the currency of agreement & shall survive even after expiry of the agreement or project.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by Their duly authorized officers or representatives.

For and on behalf of
ERNET India
Ministry of Electronics and
Information Technology,
Government of India.

For and on behalf of
<< Contractor Name >>

Name: Sh. Arun Kumar Singh
Designation: Registrar
ERNET India, Delhi

<< Authorized to sign from Contractor Name >>
Designation:
Address:

FORMATS

Format 1.1: Bank Guarantee Format for Performance Security

MODEL BANK GUARANTEE FORMAT FOR PERFORMANCE SECURITY

(To be stamped in accordance with stamp Act)

(The non-judicial stamp paper should be in the name of issuing Bank)

B.G. NO. _____
Date of issue _____
Amount (Rs.) _____
Valid upto _____
Claim Amount upto _____

To,
Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park, Delhi-110053

Dear Sirs,

In consideration of the ERNET India, Ministry of Electronics & Information Technology (hereinafter referred as the '**Owner**', which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns) having awarded to M/s. _____ (name, constitution and address) (herein referred to as the '**Contractor**', which expression shall unless repugnant to the context of meaning thereof, include its successors, administrator, executors and assigns) a Purchase Order No. _____ dated _____ valued at _____ (hereinafter referred to as Contract) and the Contractor having agreed to provide a Bank Guarantee towards Performance of the entire Contract equivalent to Rs. _____ (amount of BG) (i.e. ____ per cent of the said value of the Contract) to the Owner.

We _____ (name of the Bank) having its Registered Office at _____ and Corporate/Head Office at _____ (hereinafter referred to as the '**Bank**', which expression shall, unless repugnant to the context or meaning thereof, include the successors, administrators, executors and assigns) do hereby guarantee and undertake to pay at any time up to _____ (day/month/year including claim period) an amount not exceeding Rs. _____, within ten (10) calendar days from the date of receipt by us on first written demand by Owner; through hand delivery or registered A.D. Post or by speed post or by courier, stating that "Contractor" has failed to perform its obligations under the Contract. Aforesaid payment will be made without any demur, reservation, contest, recourse or protest and/or without any reference to the Contractor. Any such demand made by the owner the Bank shall be conclusive and binding notwithstanding any difference between the Owner and Contractor or any dispute pending before any court, tribunal or any authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the Owner and further agrees that the guarantee herein contained shall continue to be enforceable till the Owner discharges this guarantee. The owner shall have the fullest liberty, without affecting in any way the liability of the Bank under this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Contractor, and to exercise the same at any time in any manner, and either to enforce or to

forebear to enforce any covenants, contained or implied, in the Contract between the Owner and the Contractor or any other course of or remedy or security available to the Owner. The Bank shall not be relieved of its obligations under these presents by any exercise by the owner or by any other matters or thing whatsoever which under law would, but for this provision, have the affect of relieving the Bank. The Bank also agrees that the Owner 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 Contractor and notwithstanding any security or other guarantee that the Owner may have in relation to the Contractors liabilities.

This Guarantee can be invoked in one or more trenches and in such a case Owner will not be required to submit the original Guarantee along with submission of claim.

Notwithstanding anything mentioned herein above our liability under this guarantee is restricted to Rs. _____ and it shall remain in force up to and including _____ shall be extended from time to time for such period as may be desired by the Contractor on whose behalf this guarantee has been issued.

WITNESS
Signature _____
Name _____

BANK
Signature _____
Name _____

(Bank's Rubber Stamp)

Seal, name & address of the Bank and address of the Branch

Designation with Bank Stamp

Format 1.2: No Claim Certificate

(Refer Clause 12.3.1 of GCC)

(On company Letter-head)

Contractor's Name _____

[Address and Contact Details]

Contractor's Reference No. _____ Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
Shastri Park, Delhi-110053

No Claim Certificate

Sub: Contract/ Agreement no. ----- dated -----

We have received the sum of Rs. (Rupees _____ only) as final settlement due to us for the above mentioned contract agreement.

We have received all the amounts payable to us with this payment and have no outstanding dispute of any description whatsoever regarding the amounts worked out as payable to us and received by us.

We hereby unconditionally and without any reservation whatsoever, certify that we shall have no further claim whatsoever, of any description, on any account, against the ERNET India, under contract above. We shall continue to be bound by the terms and conditions of the contract agreement regarding its performance.

Yours faithfully,

Signatures of contractor or

officer authorised to sign the contract documents.

on behalf of the contractor

(company Seal)

Date: _____

Place: _____

Format 2: Authorization for Attending Pre-bid Conference.

(on Company Official Letter Head)

Bidder's Name _____

[Address and Contact Details]

Date.....

To

Registrar & CPO
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
Shastri Park, Delhi-110053

Ref: Tender Document No. Tend No./ xxxx;

Subject: Authorization for attending Pre-bid Conference on _____ (date).

Following persons are hereby authorized to attend the Pre-bid Conference for the tender mentioned above on behalf of _____ (Bidder) in order of preference given below.

Sr.	Name	Government Photo ID Type/ Number
I.		
II.		
Alternate Representative		

Note:

1. Maximum of two representatives shall be permitted to attend the Pre-bid meeting..

Signatures of bidder

or

Officer authorized to sign the bid.

Documents on behalf of the bidder

[name & address of Bidder and seal of company]

Page Left Blank Intentionally

Form 11 Financial Bid (BoQ)

Financial Bid (BoQ) <i>(This duly filled sheet must be uploaded under "upload Financial Document" tab on GeM Portal.)</i>										
Bidder Name										
Tender No										
Part A (CAPEX - I)										
Sl. No.	ITEM		Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
			(A)	(B)		(C)	(D)	(E)	F (=C+E)	G= (AxF)
1	Server Category-1		165	no.						
2A	Bidder must quote either 2A or 2 B with total HDD of 31500 HDD with each HDD of 18 TB	Server Category-2 (4U) with 60 HDD in Each Server	525	no.						
2B		Server Category-2 (6U) with 84 HDD in Each DAS	376	no.						
3	Server Category-3		30	no.						
4	Server Category-4		30	no.						
5	Server Category-5		15	no.						
6	Server Category-6		200	no.						

Sl. No.	ITEM	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
7	Server Category-7	6	no.						
8	Server Category-9	20	no.						
9	Server Category-10	16	no.						
10	Server Category-11	12	no.						
11	Server Category-13	8	no.						
12	Server Category-14	2	no.						
13	Server Category-16	2	no.						
14	DC Spine Switch	2	no.						
15	DC Leaf Switch	110	no.						
16	DC Core Switch	4	no.						
17	DC OOB Access Switch	140	no.						
18	Layer-3 Access Switch	20	no.						
19	DC CE Router	2	no.						
20	DC Border Leaf Switch	2	no.						
21	DC Internet Router	2	no.						
22	DC Interconnect Switch - Type 1	2	no.						
23	DC Interconnect Switch - Type 2	2	no.						
24	DC WAN Switch	2	no.						
25	SFP-10G-SR4	6200	no.						
26	SFP-10G-LR4	100	no.						
27	QFSP 28 -SR4	850	no.						
28	QFSP-28-LR4	10	no.						

Sl. No.	ITEM	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
29	Remote Router cum Firewall	240	no.						
30	Internet Firewall with IPS	2	no.						
31	DC Internal Firewall	2	no.						
32	DC Solution Firewall	2	no.						
33	AAA Appliance	2	no.						
34	Load balancer	2	no.						
35	Network Detection & Response (NDR)	2	no.						
36	IPS&IDS	4	no.						
37	SSL VPN Gateway	4	no.						
38	Active Directory Solution	4	no.						
39	Console management server	4	no.						
40	KVM Console	61	no.						
41	Portable KVM console adapter	15	no.						
42	Monitoring and management tool for servers	2	no.						
43	Fireproof Vault (200litre)	4	no.						
44	Degausser	5	no.						
45	Data Diode	10	no.						

Sl. No.	ITEM	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
46	Intelligent Cabling (includes all required accessories briefed in specs for 70 Racks in DC).	1	no.						
47	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 70 Racks in DC . One Monitor can maximum monitor 2 Racks	35	no.						
48	Intelligent (AIM) system Software for DC as per Spec at s.n 48	1	no.						
49	Intelligent Cabling (includes all required accessories briefed in specs for 50 Racks in DC) -Specifications similar to s.n. 46	1	no.						
50	AIM System Monitor at Rack level (Networking and Server Racks) For monitoring of 50 Racks in DC . One Monitor can maximum monitor 2 Racks- Specifications similar to s.n. 47	26	no.						

Sl. No.	ITEM	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
51	Intelligent (AIM) system Software for 10k Ports in DR-Specifications similar to s.n. 48	1	no.						
52	Smart Single Rack (minimum usable space 24U)	10	no.						
53	Non Smart Rack with Redundant IPDU	5	no.						
54	65 Inch LED Display	2	no.						
55	Heavy Duty Workstation	35	no.						
56	Heavy Duty Laptop	30	no.						
57	Heavy Duty Color Printer	4	no.						
58	Privileged Access Manager (in HA Mode)	2	No.						
59	Any other Item								
Sub Total Value of Part A (CAPEX -I)									

Part B (CAPEX - II)									
S/ N	Item	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
		(A)	(B)		(C)	(D)	(E)	F (=C+E)	G= (AxF)
1.a	<p>Data Center Infrastructure Management (DCIM), RLPAT Solution & Heat Humidity Sensor Solution Supply, Installation , Commissioning & Testing (SITC) of following:</p> <p>i) DCIM, ii) RLPAT Solution and iii) Heat-Humidity Sensor Solution with respective hardware (servers) in a High Availability mode & overall integration as per scope of work & technical specs.</p> <p>Perpetual Licenses for above solutions for :</p> <p>Number of Racks at DC = 100 Number of Racks at DR = 50 Total IT active devices at DC = 1450 , Total IT active devices at DR = 350 * Note: SI must refer to scope of work & technical specs & accordingly provide one instance of solution at DR .</p>	1	set (both working together to form HA mode*)						

S/ N	Item	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
1.b	RF Id based Physical Asset Tracking Tags with one on each IT Element (Network/servers) at DC & DR as per scope of work & technical specs.	1800	nos.						
1.c	RF Id Rack Identifiers as a part of Physical RF Id based Asset Tracking Solution at DC & DR .	150	nos.						
1.d	RF Id Based Heat and Humidity Sensors for Racks at DC & DR as per scope of work & technical specs. Note: should include sensors tags for Phase-1 equipment at DC as well.	450	nos.						
1.e	1. Communication Gateways for Communication on RF with Asset and Heat-Humidity tags & on ethernet/WiFi with respective Software Solution at DC and DR (Based on number of Asset and Heat-Humidity sensors provided.) 2. Compatible Handheld scanner to read barcode / QR codes at DC & DR 3. Barcode Printer / QR codes with consumables(3Yrs Duration) at DC & DR	2	set						

S/ N	Item	Equipment Quantity	Unit of Measurement	Make & Model	Unit Price in INR	Rate of GST in %	Amount of GST in INR	Total unit Price with GST in INR	Total Price with GST in INR
2	<p>EMS Solution (SITC of EMS (fault, performance , configuration , change , event ,traffic, asset, SLA management, IT helpdesk / service desk and IPAM functionality along with respective hardware (servers)) in High Availability mode & including the overall integration as per scope of work & technical specs.)</p> <p>Note : Solution must maintain historical data for 1 year, has an integrated syslog to acts as a sysLog aggregator. Total IT Elements = 2800 ; For 50 Concurrent Users, For monitoring of MPLS Link of 250 locations * SI must refer to scope of work & technical specs & accordingly provide one instance of solution at DR .</p>	1	set (both working together to form HA mode*)						
3	Additional EMS License Price for 50 IT devices	50	no.						
4	Additional IT Helpdesk/EMS License for 5 concurrent users	5	no.						
5	Additional DCIM User License price for 5 concurrent users.	5	no.						
6	Additional DCIM License price for 5 Racks	5	no.						
Sub Total Value of Part B (CAPEX -II)									

Part-C (OPEX)						
S/N	Item	Unit	Unit Price on Yearly basis in INR	Rate of GST in %	Amount of GST in INR	Total Yearly Price with GST in INR
		A	B	C	D	E= A X (B+D)
1	Operation and Maintenance (O&M) of DC along with deployment of 20 Technical Manpower at DC	1				
2	Operation and Maintenance of DR along with deployment of 14 Technical Manpower at DR	1				
3	Operation and Maintenance of Remote Sites	247				
4	Deployment of 2 Technical Manpower for Technical Support at Delhi	1				
Sub Total Value of Part C (Total OPEX Value)						

Summary of Price:

S/N	Description	Total Price Including GST in INR
1	Sub Total Value of part A (CAPEX - I)	
2	Sub Total Value of Part B (CAPEX - II)	
3	Sub Total Value of Part C (OPEX)	
	Grand Total Value (A+B+C)	