EOI DOCUMENTFOR

SELECTION OF SYSTEM INTEGRATOR FOR OPERATION AND MAINTENANCE AND EXPANSION OF PHYSICAL AND IT INFRASTRUCTURE FOR DATA CENTRE

EOI   No: ITI/RODEL/2K22/MSPD/SDC/03

Date of Issue: 20.10.2022

Issued By:
AGM (Marketing & Purchase)
Telefax: +91 (11) 22050998
https://www.itiltd.in/

	ITI Limited (A Govt. of India Enterprise) ITI Limited, MSP-Delhi Core-1 Floor-11 Scope Minar Laxmi Nagar, New Delhi-110092 **Telephone no.: +91 (11) 22050998** **website:** https://www.itiltd.in/ **Email: etenderiti_mspdli@itiltd.co.in**	

SECTION-1

EXPRESSION OF INTEREST (EOI)

ITI Limited is a Govt. of India Undertaking organization under the Ministry of Communication & IT engaged in ICT business along with other diversifying business areas.

This RFP/Tender is aimed at identifying suitable Organization as a 'System Integrator' having adequate strength in the field of Data Center and Cloud computing.

The 'System Integrator' (SI) shall act as a backend partner of ITI to execute the project in India. All mission critical activities would be managed and supervised by ITI through its experienced Managers and qualified Professionals in the respective areas.

With this vision and commercial objective, sealed bid is invited for the above-mentioned work. The Sealed Technical and Financial proposal under Two Cover-System may be submitted by the Bidder(s). It is must for the bidders to meet the Eligibility Criteria as mentioned in the RFP/Tender document.

Submission of Online Bids is mandatory for this EOI. Prospective bidders need to submit their bids with the most competitive Techno-commercial offer for the aforesaid work. EOI document is available on ITI website (https://tenders.itiltd.in/) , CPP publishing portal & Tender Wizard portal. The important dates are as given below:-

1.1   IMPORTANT DATES

Date of Posting of EOI:	[20.10.2022]
Start Date of downloading/viewing EOI:	[20.10.2022]
Start date & time for Online submission of Bids:	[21.10.2022], [10:00 hrs]
Last date & time for Online submission of Bids:	[31.10.2022], [12:00 hrs]
Online Opening of Technical Bid (Part-I):	[31.10.2022], [13:00 hrs]
Online Opening of Financial Bid (Part-II):	To be notified later

Bids shall be submitted on Tender Wizard portal. Bidders are advised to visit Tender Wizard portal and/or ITI website regularly for updates/amendments, if any. Bidders require any clarification please contact helpdesk:
1. Prashant Kumar, CM-NT; +91-99100-48364
2. Abhay Sharma, Executive (M); +91-78274-50462

1.2   ELIGIBILITY CRITERIA

- The bidder should be a company registered under the Companies Act, 1956 since last 3(three) years.
- Bidder should have experience of IT System Integration/ Information Technology Infrastructure projects including implementation / operations and should have been in this business for a period exceeding three years as on 31.03.2021.
- Bidder who has acquired a company/division of a company having experience as mentioned above shall also be considered
- The bidder must have ISO 9001: 2015 Certificate.
- The bidder shall fulfill the following financial criteria: -

    i.   Bidder shall have Average Annual Financial Turnover during the last 3 financial years, ending 31st March of the previous financial year should be at least 30% of the total quoted price (Total cost of the quoted packages) (excluding GST)

    ii.   Net worth should be positive as on 31st March of last Financial Year.

- Experience of having successfully commissioned and installed during the last 10 years from the date of bid submission should be either of the following:-

  Three similar works each costing not less than 10 Cr of the in last 5 years.

  OR

  Two similar works each costing not less than 13 Cr in last 5 years.

  OR

  One similar work costing not less than 20 cr in last 10 years.

  Considering following requirements:
  a) An order (including IT and Non-IT but excluding basic building structure) should be there
  b) Valid BS 7799 / ISO 27001 / ISO 20000 certification.
      Note:
      • Bidder's in house data centers shall not be considered.
      • Bidders who have built their own Internet Data Centre (IDC), for commercial use will be considered.

- The bidder should have experience in providing Facility management services to at least one data center, for the last three years i.e. 2017- 2018, 2018-19 & 2019-20 Note: The Facility management services shall include IT infrastructure related (e.g. Servers, Storage, networks etc.)/ non IT related services (power, cooling, physical security etc.)
  i. Bidders who have built their own Internet Data Centre (IDC), for commercial use will be considered.
  ii. Bidder's in house data centers shall not be considered.
- Bidder must have on its roll at least 100 technically qualified professionals in the area of networking, systems integration & prior experience in providing the Data Center Infrastructure maintenance services as on 31.03.2021.
      A) At least two resources should be ITIL certified
      or
      B) ISO 27001 2013/ ISO 20000:2018 LA certified/CDCE/CDCS.
- The bidder should have a valid PAN and GST Registration (copy of PAN card and GST Registration certificate should be submitted in the bid). Copy of PAN card and GST Registration certificate should be submitted in the bid.
- The bidder shall not be under a declaration of ineligibility for corrupt or fraudulent practices or blacklisted with any of the Government agencies.
- The bidder should submit furnish an **EMD of Rs. 30,00,000.00/- (Thirty Lac)** and Tender Fees of **Rs. 10,000.00/- (Ten Thousand)** in form of RTGS to below mentioned Account Details:
  i. Online RTGS/ NEFT
  ii. Bank: Bank of Baroda, KG Marg
  iii. MICR: 110012021
  iv. IFSC: BARB0CURZON
  v. Acc. No.: 06230500000010
- **Manufacturers Authorization Certificate (MAF)**

  i. The bidder should submit Manufacturers Authorization Certificate (MAF) from Original Equipment Manufacturers (OEMs) specific to the bid for items mentioned in this EOI.
  ii. Bidder should Confirm that the products quoted are not "end of life or end of sale products" as on Bid Submission date. If in case the support for the product quoted has been stopped/ withdrawn till the time of delivery of equipment, the same will be changed with the equivalent or superior product at no extra cost.
  iii. Bidder should Undertake that the support including spares, patches, and upgrades for the quoted products shall be available for 7 years from the signing of contract
  iv. Bidder should submit valid letter from the OEMs for each product to be used in datacenter in the format as attached annexure II.
  v. The bidder should not be insolvent, in receivership, bankrupt or being wound up, not have had theirbusiness activities suspended and not be the subject of legal proceedings for any of the foregoing. An undertaking by the bidder should be submitted.

vi.   The Bidder should not be blacklisted/debarred/banned/restricted by any Union Govt./State Govt./PSU as on date of submission of the Bid. "No-Conviction Certificate" duly signed by authorizedsignatory signing the bid, should be submitted in the prescribed format.

- The bidder needs to submit un-priced BOQ along with their technical bid.

- The bidder needs to submit an Undertaking stating that: Vendors, whose Purchase Order(s) for any Project of ITI was/were cancelled on risk & cost basis for non-performance or non-submission of performance guarantee in last 2 years, are not eligible to participate in this tender.

- The selected bidder should have an office in the state. However, if the local presence is not there in the state, the selected bidder should give an undertaking for establishment of an office, within two months of award of the contract.

- No consortium and subcontracting is allowed.

OEM Qualification Criteria

Qualification criteria for OEM	
	1. Existence in India for more than 10 years - Self certification fromOEM must be submitted
	2. Average annual turnover of INR 800 Cr for OEM of Servers in India and INR 500 Cr for OEM of Storage, for last 3 years from product sales – CA Certificate to be submitted
	3. Should have supplied their similar category of proposed products in at least 5 Data Center projects implemented in the last 5 years - PO/Contract Proof should besubmitted Should provide 100% Data operation - Self certification fromOEM must be submitted
	4. Proposed OEM of Networking should have minimum 5 Spare Depots spread across India - The spare depot list to be provided, which should be legally signed by the OEM legal entity.
	5. Proposed OEM of Networking must have ISO9001, ISO 14001 - Valid ISO Certificates to be given
	6. Should be Financially Profitable for past 3 years - CA Certificate to be submitted
	7. Should have supplied their similar category of proposed products in at least 5 Data Center projects implemented in the last 5 years - PO/Contract Proof should besubmitted
	8. All the Networking products proposed should be supported bya "Malicious code free" Authorization Letter legally vetted by the OEM - Self declaration to be given by OEM
	9. Proposed OEM should have presence in India for the past 10 years - Self declaration to be given by OEM
	10. The Security OEM must have its own operational SOC anywhere across the Globe - Self declaration to be given by OEM OEM should not be blacklisted by any sovereign government / central / State / UT Government or Govt PSU as on the date ofsubmission of bid – Self Declaration from OEM should be submitted

- **LABOUR LAWS (wherever applicable):**

The Bidder should comply with all applicable Indian Labor laws, Payment of Minimum Wages

Act, Workman's Compensation Act, EPF/ESI provisions and any such statutory provisions. In case the bidder is found to be not complying to any of the relevant statutory requirement, action as deemed fit may be initiated by ITI at its sole discretion.

1.3   The bidder should give an undertaking on the company's letter head that all the documents/certificates/information submitted by them against this EOI are genuine.

In case any of the documents/certificates/information submitted by the bidder is found to be false or forged, ITI shall immediately reject the bid of such bidder(s) or cancel/terminate the contract and forfeit bid security / Performance Security submitted by the bidder and debar them from participation infuture EOIs/tenders of ITI for a period upto 3 years.

1.4   A statement showing Clause-by-Clause compliance to all Terms & Conditions of all the Sections of this EOI as well as client's tender (which forms part of this EOI), duly Signed and Stamped on the Letter Head of their Organization. The bidder shall submit No-Deviation Certificate along with above.

Bidder shall submit technical data sheet by highlighting each complied specification. Wherever technical specifications and operational/functional requirements not mentioned in datasheet, OEM compliance shall be submitted.

1.5   BID SECURITY (EARNEST MONEY DEPOSIT)-

The bidders shall furnish an EMD of Rs. 30,00,000.00/- (Thirty Lakh Only) in form of RTGS as mentioned above in documents.

Note:- Bids received without EMD and tender fees shall be summarily rejected..

1.6   TENDER FEES:

The bidder shall furnish tender fees of Rs. 10,000.00/- (Ten Thousand Only) in form of RTGS as mentioned above in documents.

1.7   EVALUATION

1. This RFP/Tender would be subjected to a Two Stage (Technical & Commercial) Evaluation Process. All the Bidders are requested to note the entire evaluation process carefully.

2. Prior to the detailed evaluation, ITI will determine the substantial responsiveness of each Bid to the RFP/Tender Document. For the purpose of ascertaining the eligibility,

3. A substantially responsive bid is one which confirms to all the terms and conditions of the RFP/Tender Document without deviations.

4. The purchaser's determination of bid's responsiveness shall be based on the contents of the bid itself without recourse to extrinsic evidence.

5. ITI may waive any minor infirmity or non-conformity or irregularity in the bid which doesn't constitute a material deviation, provided such waiver doesn't prejudice or effect the relative ranking of any bidder. The bids submitted by the Bidders would be subjected to a well-defined and transparent evaluation process.

6. The Bids would be evaluated by a duly constituted Committee of ITI Limited, whose decision would be taken as final.

7. The Bidders who have submitted the RFP/Tender Document cost only those bidders will be considered for Technical Evaluation.

8. In Technical Evaluation process, all the Technical Bids of the preliminary eligible bidders (as mentioned above) would be scrutinized thoroughly w.r.t. our EoI/RFP/Tender Document. The Bidders, who will qualify in the Technical Evaluation process, would be considered for Commercial Evaluation.

9. In Commercial Evaluation process, all the Commercial Bids of the technically qualified bidders (as mentioned above) would be scrutinized thoroughly w.r.t. our RFP/Tender Document.

10. The evaluation methodology will be distributed in two parameters.

>   a. Technical Evaluation
>   b. Financial Evaluation

11. LCBS will be performed.

A= Total Cost Quoted without taxes
B= Quoted Margin to ITI (Percentage of A)
C (Absolute value of margin) = $(A*B)/100$
D (Overall Quoted Price) = A-C

12. The Bidder with lowest value of D will be termed as successful

13. The Bids having higher value of B should be selected in case of tied 'D'

14. ITI reserves the right to reject any or all bids without assigning any reasons thereof.

1.8   VALIDITY PERIOD OF BID

Bid shall remain valid for 200 days after the date of bid opening. The bid valid for a shorter period shall be rejected as non-responsive. In exceptional circumstances, ITI may request the bidder for an extension to the period of bid validity if same is extended by end client and accordingly, the bid securityshall also be suitably extended by the bidder.

1.9   NON-DISCLOSURE OF CONTRACT DOCUMENTS:

Except with the written consent of the Buyer/ Seller, other party shall not disclose the contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party

1.10 AUTHORIZATION LETTER/ BOARD RESOLUTION:

The bidders need to submit board resolution along with authorization Letter in Online mode authorizing the signatory to act on behalf of the bidder. The Authorized person should be either authorized by Board or a employee authorized by one of the following person who has the Board Resolution to delegate authorization to other:

1.   Managing director
2.   The Chief Executive Officer
3.   The manager;
4.   The Company Secretary
5.   The Whole-time director
6.   The Chief Financial Officer

The bidder should ensure that the Digital Signature used for uploading the tender document in e tender

portal should be of the authorized signatory.

1.11   MOU/AGREEMENT

Selected bidder will have to sign MoU with ITI.

1.12   SUBMISSION OF FORGED DOCUMENTS

Bidders should note that ITI may verify authenticity of all the documents/certificate/information submitted by them against the EOI. In case at any stage of this process, if it is established that bidder has submitted forged documents/certificates/information towards fulfillment of any of the EOI/contract conditions, ITI shall immediately reject the bid of such bidder(s) or cancel/terminate the contract and forfeit bid security / Performance Security submitted by the bidder and debar them from participation in future tenders of ITI for a period upto 3 years.

1.13   CONTACT INFORMATION

CM NT:	**M (E)**
[Prashant Kumar]	**[Abhay Sharma]**
Mb.: +91-99100-48364	Mb. - +91-78274-50462
e-mail: prashant_rodel@itiltd.co.in	e-mail: abhaysharma_crp@itiltd.co.in

END OF SECTION-1

SECTION-2

GENERAL TERMS & CONDITIONS OF THE CONTRACT

The prospective bidders are advised to study the EoI carefully. Submission of youroffer/bid shall be deemed to have been done after careful study and examination of the EOI with full understanding of its implications. Failure to furnish all information required in the EOI or submission of an offer/bid not substantially responsive to EOI in every respect will be at the Bidder's risk and may result in its outright rejection.

The Bidder shall bear all costs associated with the preparation and submission of its Bid, including cost of presentation for the purposes of clarification of the Bid, if so desired by ITI Limited. In no case, ITI would be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering Process. ITI reserves the right, not an obligation, to carry out the capability assessment of the Bidder(s). This right inter alia includes seeking Technical-Demonstrations, Presentations, Proof of Concept and Live-site visits etc.

1	**Empaneled Vendor of ITI**	NA (Open Tender)
2	**Non-transferable Offer**	This EoI/RFP/Tender document is not transferable. Only those, who have paid the tender fees, are entitled to quote.
3	**Only one Proposal**	The Bidder should submit only one Bid/Offer/Proposal. If the Bidder submits or participates in more than one proposal, such proposals shall be Disqualified.
4	**Language of the Bid**	All information in the Bid, correspondence and supporting documents, printed literature related to the Bid shall be in English. Failure to comply with this may disqualify a Bid. In the event of any discrepancy in meaning, the English language copy of all documents shall govern.
5	**Clarification and Amendment in Tender**	At any time before the submission of Proposals, ITI may amend the RFP/Tender document by issuing an addendum / corrigendum in writing or by standard electronic means. The addendum / corrigendum will be uploaded on the website. Please visit regularly the Tender Wizard portal.
6	**Amendment to Bid**	At any time prior to the deadline for submission of bids, the bidder may, for any reason, whether at its own initiative, or in response to a clarification requested by a prospective Bidder, submit the Revised Financial Bid.
7	**Modification and Withdrawal of Bid**	No bid may be withdrawn or modified in the interval between the bid submission deadline and the expiration of the bid validity period specified in Bid documents. Modification or Withdrawal of a bid during this interval will result in the forfeiture of its bid security/ Appropriate action.
8	**Validity of Offer**	The offer should be valid for a minimum period of 200 days

9	**Prices**	The prices quoted by the Bidder shall be FIRM and final and no amendment/ alteration to the rate quoted in tender will be accepted at the later date. A bid submitted with an adjustable price quotation will be treated as non-responsive and Rejected. Term of Price: Bidder must quote the rate on FOR destination basis in Indian Rupees Only
10	**Deviation Clause**	No Deviation from Specifications, Terms & Conditions of the tender is allowed. Quotations having deviation from our specifications, standard terms & conditions would be liable to be rejected. Conditional bid is subject to rejection.
11	**Taxes and duties**	The taxes and duties are to be clearly mentioned, if any. No extra charge/ taxes over and above the quoted rate in any form will be borne by ITI. Back to Back basis.
12	**Delivery schedule**	SI have to operate and maintain the SDC for a period of 5 years from the date of Go Live of SDC post completion of expansion
14	**Payment Terms**	a) Back to Back basis (As per the customer's contractual guidelines) b) No advance payment will be made
15	**Warranty / Annual Maintenance Contract (AMC)**	5 years Warranty
16	**Liquidated Damages (LD)**	Liquidated Damages and Penalty shall be levied on back- to-back basis i.e. ITI shall deduct from the payment on amount equal to the LD levied on ITI by the end customer.
17	**Training**	As per customer requirement
18	**Acceptance Test Procedure (ATP)**	a) SI have to conduct the Acceptance Test (AT) before handing over ofthe project(s) to end customer. b) End Customer will perform testing.
19	**Damage to Properties**	In case of any accident/damage to customer/end user properties by the vendor, full responsibility will be attributed to the vendor.
20	**Contractual Period**	As per customer requirement
21	**Extension of Contract**	On back-to-back basis.
22	**Inspection Authority**	End Customer
23	**Tender Award Criteria**	Bidder Technical and Financial capabilities will be evaluated by a committee nominated comprising of internal stake holders of ITI Limited. Lowest Cost based Selection will be done
24	**Tender Document Cost**	**In case of bid submission:** Tender Document Cost (Nonrefundable) must be remitted through NEFT/RTGS/Net Banking. **The Bank Details of ITI Limited for NEFT/RTGS/Net Banking is as below:** Online RTGS/ NEFT Bank: Bank of Baroda, KG Marg MICR: 110012021 IFSC: BARB0CURZON Acc. No.: 06230500000010

25	**Performance Security Deposit**	An unconditional and irrevocable and continuing Bank Guarantee for Contract Performance (3 % of the total contract value) OR Back to Back basis
26	**Consortium Bidding**	Not Allowed.
27	**Signing of theBids**	The Bid must contain the name, place of business of the person orpersons making the Bid and having Power of Attorney and must be signed & submitted by the Bidder with his usual signatures. Satisfactory evidence of authority of the person signing the bid on behalf of the Bidder shall be furnishedon non-judicial stamp paper of an appropriate value with the Bid in the form of a **Power of Attorney**, **duly notarized by a Notary Public**, indicating that theperson(s) signing the bid have the authority to sign the bid and that the bid is binding upon the Bidder during the full period of its validity. All the pages of Bid document and supporting documents must be signed and stamped by the authorized signatory having Power of Attorney. Any interlineations, erasures oroverwriting shall only be valid if they are initialed by the signatory (ies) to the bid.
28	**Submission of Tender**	The '**Technical Bid**' and **'Commercial Bids'** shall be submitted in ITI Limited Tender Wizard Portal before due date and time.
29	**Opening of Tender**	Technical bid will be opened on due date of tender opening. **Note** 1: The bidders or their authorized representatives may also be present during the opening of the Technical Bid, if they desire so, at their own expenses. **Note 2**: The technical bids will be opened and evaluated by a duly constituted committee. After evaluation of the technical bid, Price bids of only those bidders will be opened whose technical bids are found suitable. Intimation of opening of financial bid will be given to the technically qualified bidder accordingly.
30	**Rejection of Bid**	ITI reserves the right to reject any or all tenders/quotations/bids receivedor accept any or all tenders/quotation/bids wholly or in part. Further, ITI reserves the right to order a lesser quantity without assigning any reason(s) thereof. ITI also reserves the right to cancel any order placedon basis of this tender in case of strike, accident or any other unforeseencontingencies causing stoppage of production at ITI or to modify the order without liability for any compensation.
31	**Termination ForDefault**	ITI may terminate the contract in whole or in part for the following reasons: • If the bidder fails to deliver any or all of the goods/services within the period(s) specified in the contract/purchase order, or within the extension time granted by ITI. • If the bidder fails to perform any other obligation(s) under the contract/purchase order. • If the bidder has engaged in corrupt/fraudulent practices in completing/executing the work assigned to him. • ITI may, without prejudice to any other right or remedy available to it, by a three days' notice in writing, can terminate the contract as a whole or in part in default of the contract. ITI shall have the right to carry out the incomplete work by any means at the risk andcost of the bidder.

		• In addition to rights to forfeiture of PBG and application of LD charges, on the cancellation of the contract in full or in part, ITI shall determine what amount, if any, is recoverable from thecontractor for completion of the work or part of the works or in casethe works or part of works is not to be completed, the loss or damage suffered by ITI. In determining the amount, credit shall begiven to the contractor for the value of the work executed by him up to the time of cancellation, the value of contractor's material taken over and incorporated in work assigned as per the purchase order. • "Corrupt practices" means the offering, giving, receiving or soliciting of anything of value to influence the action of public official in the procurement process or in contract execution.
		"Fraudulent practices" a misinterpretation of facts in order to influence the action of a public official in the procurement process or in contract execution and includes collusive bidding among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels to hamper free and open competition.
	Force Majeure	Neither party shall bear responsibility for the complete or partial non-performance of any of its obligations, if the non-performance results from such Force Majeure circumstances i.e. Flood, Fire, Earth Quake, Epidemic and other acts of God as well as War, Military Operation, Blockade, Act or Actions of State Authorities that have arisen after signing of the present contract. Party invokingthis clause shall serve notice of seven days along with the proof of occurrence of the force majeure event to the opposite party. At the time of cessation of such force majeure event a notice of the same shall also be served to the opposite party. In such circumstances, upon a written approval of ITI, the time stipulated for the performance of an obligation under the present contract will stand extended correspondingly for the period of time of action of these circumstances and their consequences. However,any such extension shall be given only if extension is granted by theultimate buyer/ user. Parties at all times take reasonable steps within their respective powers and consistent with good operation practices (but without incurring unreasonable additional costs) to: a) Prevent Force Majeure Events affecting the performance ofthe Company's obligations under this agreement; b) Mitigate the effect of any Force Majeure Event; and c) Comply with its obligations under this agreement. d) Further if the period of Force Majeure event extends beyondthree months the parties may consider the fore closure of theagreement. * Period of three months may vary at the discretion of ITI as per thevalidity period of the contract.
33	**Arbitration**	All disputes arising out of this contract shall be referred to the sole arbitration of MSP Head, ITI Limited, Delhi or his nominee as per the Provisions of Indian Arbitration and Reconciliation Act 1996. Decision of arbitrator shall be final and binding on both the parties.

34	**Jurisdiction**	This contract between the supplier and buyer shall be governed by the laws of India and this contract shall be taken up by the parties for Settlement and orders only in Delhi jurisdiction.
35	**Manpower Support**	Manpower Support for whole contract period: To maintain the functionality of the integrated EACS, two qualified technicians shall be provided by the firm on site (one each from 0800hrs- 1500hrs and 1400-2000 hrs., Mon to Sat). They will test the functional status of various deployed equipment in the entire premise starting at 0800 hrs. daily and, will maintain a log. At least one technician will be available at site for support from 0800- 2000 hrs.
36	**Other Terms and Conditions**	
i.		The Bidder(s) are required not to impose their own terms and conditions to the bid and if submitted, it will not be considered as forming part of their bids. The decision of ITI shall be final, conclusive and binding on the Bidder(s).In a nutshell, the Conditional Bid or Bid with deviations will be summarily rejected.
ii.		The Bids/Offers of the Qualified bidders (who qualify the eligibility conditions) only would be subjected to the technical-evaluation.
iii.		The bidder is expected to go through the Scope of work and Specifications. The bidders are to quote only fully compliant solution.
iv.		The exact strategy to address and win the business opportunity would be shared / discussed with the **Best-Rated** qualified bidder in due course of time.
v.		The bidder is required to extend the requisite support during the evaluation by giving Technical Presentation /Demonstration /Arranging site visits (if required) on "No-Cost No-commitment" basis.
vi.		Any clarification issued by ITI in response to query raised by prospective bidders shall form an integral part of bid documents and it shall amount to an amendment of relevant clauses of the bid documents.
vii.		A clause-by-clause compliance statement to all Sections of the RFP/Tender document is to be submitted in the Technical Bid, demonstrating substantial responsiveness. A bid without clause-by-clause compliance statement to Eligibility Criteria of the RFP/Tender document, shall not be considered for evaluation and shall be summarily rejected.
viii.		The bidder should study carefully the document to assess the work and Risk factors associated with such type of Business opportunities.
ix.		The bidder has to consider the following major Cost Factors while arriving at a commercial decision: • Direct Cost (requisite IT Hardware and Application Software) • Fiscal Cost • Logistic-Cost • Services and Administrative Cost • Training and Documentation Cost • Contingencies
x.		The bidder should enclose the documents in their '**Technical Bid**' & '**Commercial Bid**' as specified in the tender documents.
xi.		Please note that if any document/authorization letter/testimonies are found fabricated /false/ fake, the bid will be declared as disqualified and EMD will be forfeited. This may also lead to the black-listing of the bidder.
xii.		All the required documents to establish the bidder's eligibility criteria should be enclosed with the original bid/offer (Technical-Bid) itself. The EoI/RFP/Tender will be evaluated on the basis of the documents enclosed with the original bid/offer only. ITI will not enter into any correspondence with the bidder to get these certificates/ document subsequently. However, it reserves its right to get them validated/verified at its own.

xiii.		Due to any breach of any condition by the bidder, the Bid Security (EMD) if any submitted by the bidder may be forfeited at any stage whenever it is noticed andITI will not pay any damage to the bidder or the concerned person. The bidder or/and the person will also be debarred for further Participation in future EoI/RFP/Tenders.
xv.		The training shall be given to the end customer to ensure trouble free operationsof the System/Equipment.
xvi.		The bidder is required to enclose Notarized Copy of the Power of Attorney fromits Directors/Top management which should indicate clearly the name of the signatory and title. The Bidders must ensure that all the documents are sealed and signed by authorized signatory.
xvii.		The Power of Attorney given to the Authorized Signatory should be submitted and executed on the non-judicial stamp paper of appropriate value as prevailingin the respective states(s) and the same be attested by a Notary public or registered before Sub-Registrar of the states(s) concerned.
viii.		Sealed offer/bid prepared in accordance with the procedures enumerated above should be submitted to the Tenderer not later than the date and time laid down,at the specified address.
xix.		ITI shall not be responsible for any postal delay about non-receipt / non- deliveryof the bid/documents. This EoI/RFP/Tender Document is absolutely not transferable.
xx.		The bid submitted may be withdrawn or resubmitted before the expiry of the last date of submission by making a request in writing to ITI to this effect. No bidder shall be allowed to withdraw the bid after the deadline for submission of the EoI/RFP/Tender. In case of withdrawal after deadline of submission, EMD will be forfeited.
xxi		Bidder must ensure that each page of tender document including corrigendum and offline documents needs to be submitted along with the bid failing to which the bid is liable to rejection
xxii		Any cost incurred on additional items/ system/component/ accessories required would be borne by bidder.
xxiv		All the other terms and conditions as per technical document will be imposed on the bidder.

END OF SECTION-2

SECTION – 3

SPECIAL CONDITIONS OF CONTRACT

Note: In case clauses/ sub-clauses have any difference mentioned in this EOI at different places, the conditions mentioned in this section shall prevail. The terms and conditions of this section shall be on back to-back basis based on client's requirement.

3.1 PAYMENT TERMS

Payment terms are as per end customer tender document.
No advance will be made.

3.2 PERFORMANCE SECURITY

a) The bidder will submit undertaking to submit back-to-back PBG (Performance Security) as submitted by ITI to end Client if the contract is awarded to ITI by end Client.
Bidder has to give PBG of at least 3% of the contract value or customer requirement.

3.3 PRICE BASIS

As per Client's Terms and conditions

3.4 PAYING AUTHORITY

AGM (M & P)
ITI Limited, MSP-Delhi Core-1 Floor-11
Scope Minar Laxmi Nagar,
New Delhi-110092

3.5 INSURANCE

As per Client's Terms and conditions

3.6 DELIVERY / IMPLEMENTATION SCHEDULE

As per Client's Terms and conditions

3.7 WARRANTY & AMC

As per Client's Terms and conditions

3.8 PERIOD OF CONTRACT

As per Client's Terms and conditions

3.9 TERMINATION OF CONTRACT

As per Client's Terms and conditions

3.10 PENALTY

As per Client's Terms and conditions

3.11 SLA

As per Client's Terms and conditions

3.12 UPTIME

As per Client's Terms and conditions

3.13 LIQUIDATED DAMAGES
As per Client's Terms and conditions

3.14 DELIVERY PERIOD EXTENSION :

As per client's Terms and conditions

END OF SECTION-3

<div align="center">

SECTION-4

SCOPE OF WORK & TECHNICAL SPECIFICATIONS

</div>

AS PER CLIENT's TENDER, however a brief scope is given below:

Technical Requirements

This section describes the overall IT infrastructure as well as Non-IT Infrastructure function and technical specifications for the SDC project. The bidder has to meet all these defined requirements hereunder.

SDC Architecture – IT

SDC architecture is being depicted in the schematic as:
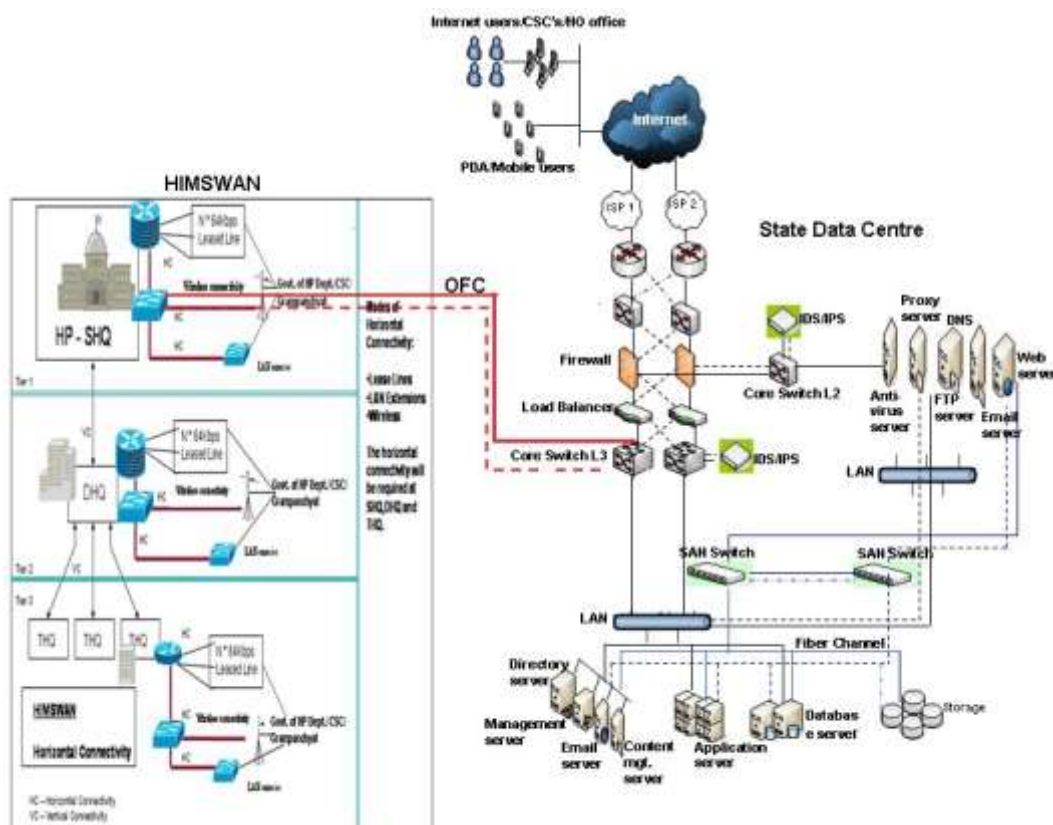
Server and Application Set-up

SDC hosts various e-governance applications, information portal, Citizen centric services applications, service delivery gateways, payment gateways and multiple databases with heterogeneous environment. In order to meet these various application servers/ systems and management software are required with perpetual full use processor license and with technical support, update and upgrade facility during five years of operation period. The major components but not limited are mentioned below:

Web Servers

Web based applications are easily accessible from any sort of the network, Intranet, internet or extranet. Therefore, Web server plays a vital role in SDC. Most of the new G2C applications are having web interfaces, which require web servers for such services. The web servers are used for web hosting for different departments. Hence servers with high availability, clustering and load balancing facility must be provided. The Volume Manager and File system should support heterogeneous Storage models from different OEMs. If, the Clustering software is provided, it should support heterogeneous Operating systems from different OEMs.

Application Server

Application in the middle tier for various web based applications. Application servers take careof the necessary workflow and web server are required for the interfacing with the end user.Both the web and app server are seamlessly integrated to provide high availability and performance. With the use of server load balancers, user requests are distributed among various clustered/common servers. There are two separate applications solutions for Unix/Linux and Windows environment. Hence servers with high availability, clustering and load balancing facility must be provided.

Database Server

The database/repository provides all the relevant information required to process any Citizen/Government request or to render any e-Governance services with the use of SDC. Database server are required to store and access data with ease. Hence servers with high availability, clustering and load balancing facility must be provided. The Volume Manager and File system on the server should support heterogeneous Storage models from different

OEMs. For Database cluster, the clustering software should support heterogeneous Operating systems from different OEMs.

Directory Server

Using Directory services SDC administrator is able to define centralized authentication & authorization mechanisms for users. This enables associate policies such as security, management etc on all servers/systems from a centralized console and enhances security, reduces IT complexity and increase overall efficiency. It also enables central authentication thus enabling single sign-on (SSO) mechanism irrespective of Operating System at client end

i.e. MS Windows, Linux etc. Therefore this user directory enables easy manageability that is creation, modification and deletion of user records. It further helps to integrate with various other services like messaging, proxy, etc. The directory services should also be able to cater the requirements of the State for Client workstations at SDC.

Firewall

A firewall is a dedicated appliance in High availability mode which inspects network traffic passing through it, and denies or permits passage based on a set of rules. A firewall's basictask is to regulate some of the flow of traffic between computer networks of different trust levels. There is a perimeter / external firewall in redundant mode which acts as layer of security for SDC IT infrastructure. Hence firewall with high availability (i.e. redundancy at ports level on different slots with internal N+1 power supply, supervisor engine) and load balancing facility must be provided.

Enterprise Management System (EMS)

The management server helps in administration of heterogeneous systems at SDC. The management server helps in efficient and reliable administration of all the computing and networking devices and enables:

1. Asset Management
2. Patch management
3. Monitor the availability of Services
4. Fault Management
5. Performance Management (Server, Network, Security, SAN etc)
6. Security information management (analyze logs of servers, network devices)

The necessary server, operating system, database and required CAL Licenses for theirmonitoring etc for EMS in SDC would be provisioned by DCO on its own and cost of the

same would be built-in the solution proposed by the DCO. No separate line items would be mentioned for these items in the BOM.

Helpdesk Management System

An ITIL based Helpdesk system is used for assisting the service delivery by DCO for SDC. Helpdesk system automatically generates the incident tickets and logs the call. Such calls are forwarded to the desired system support personnel deputed by the DCO. These personnel look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system is having necessary workflow for transparent, smoother and cordial SDC support framework.

1. Provide flexibility of logging incident manually via windows GUI and web interface.
2. The web interface console of the incident tracking system would allow viewing,updating and closing of incident tickets.
3. System should provide Knowledge base
4. Provide seamless integration to events/incident automatically from NMS / EMS.
5. Allow categorization on the type of incident being logged.
6. Provide classification to differentiate the criticality of the incident via the priority levels,severity levels and impact levels.
7. Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS or NMS.
8. Provide audit logs and reports to track the updating of each incident ticket.
9. Proposed incident tracking system would be ITIL compliant.
10. It should integrate with Enterprise Management System event management andsupport automatic problem registration, based on predefined policies.
11. It should be able to log and escalate user interactions and requests.
12. It should provide status of registered calls to end-users over email, SMS and throughweb.

The necessary server, operating system, database etc. required for the implementation of Helpdesk Management in SDC would be provisioned by DCO on its own and cost of the same would be built-in the solution proposed by the DCO. No separate line items would be mentioned for these items in the BOM. However, the DCO has to provide necessary licenses to cover all the IT infrastructure installed in the HP SDC during the operation period five years.

Intrusion Prevention System (NIPS)

Any attempts of intrusion over a network is detected, logged into a database (which forms the basis of reports generated) and further protecting the SDC infrastructure. This provides proactive information while the network is being compromised based on certain network patterns detected. All the Critical servers will be enabled with host based IPS. Hence IPS for NIPS as with high availability (i.e. redundancy at

ports level on different slots with internal N+1 power supply) and load balancing facility must be provided. The NIPS Should protect against SSL based attacks either by offloading to internal processor or by integrating with external high-capacity SSL accelerators.

Technical Specifications - IT Components

Access Switch

S. No.	General Specifications
1.1	**General Features:**
1.1.1	Switch should be 1U and rack mountable in standard 19" rack.
1.1.2	Switch should have internal hot-swappable Redundant Power supplyfrom day 1.
1.1.3	Switch should have redundant hot swappable fans.
1.1.4	Switch should have minimum 8 GB RAM and 8 GB Flash/SSD
1.1.5	Switch should have for modular stacking, in addition to asked uplink ports or should support Multi Chassis Link Aggregation
1.2	**Performance:**
1.2.1	Switch shall have minimum 3.6 Tbps of switching fabric and minimum 1.2 Bpps of forwarding rate without considering stacking performance.
1.2.2	Switch shall have minimum 32K MAC Addresses and 1000 active VLAN.
1.2.3	Should support minimum 32K IPv4 routes or more and 16K IPv6 routes ormore
1.2.4	Switch shall have 8K or more multicast routes.
1.2.5	Switch should support atleast 64K flow entries or should support sflow.
1.2.6	Switch should support 128 or more STP Instances / MSTP/VSTP instances
1.2.7	Switch should have 16MB or more packet buffer.
1.3	**Functionality:**
1.3.1	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u/802.3ab/ 802.3z & 1588v2/ PTP transparent
1.3.2	Switch must have functionality like static routing, RIP, PIM, OSPF,VRRP, PBR and QoS features from Day1
1.3.3	Should support advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF,VXLAN, IS-ISv4, OSPFv3, MP-BGP
1.3.4	Switch shall have 802.1p class of service, marking, classification, policing andshaping and eight egress queues.
1.3.5	Switch should support management features like SSHv2, SNMPv2c,SNMPv3, NTP, RADIUS and TACACS+ .

1.3.6	Switch should support IPv6 Binding Integrity Guard /IPv6 Snooping/DHCP V6 Snooping , IPv6 RA Guard, IPv6 DHCP Guard/IPV6 access security , IPv6 Neighbor Discovery Inspection/ Neighbor discovery protocol and IPv6 Source Guard.
1.3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-256 on hardware or shouldhave FIPS Compliance
1.3.8	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type or should supportVoIP Vlan support
1.3.9	During system boots, the system's software signatures should be checked forintegrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.
1.4	**Interface**
	Switch shall have 48*10/25 G SFP+, 2*40/100 G scalable to 6*40/100 G uplink Port.
1.5	**Certification:**
1.5.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
1.5.2	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CEClass A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.
1.5.3	Switch / switch series / Switch's Operating System should be tested for EAL2/NDPP or above under Common Criteria Certification.

OOB Switches

SN.	Specification
1	**General Hardware and Interface requirements**
1.1	Switch should have minimum 24x10/100/1000Mbps Ethernet Ports and 4x10GSFP+ uplink ports.
1.2	Switch shall support minimum 80 Gbps of stacking bandwidth and stacking portshould be dedicate port not uplink port
1.3	Switch should have Redundant Power supply
1.4	Stacking module should be hot-swappable.
2	**Performance Requirements**
2.1	Switch shall have minimum 128 Gbps of switching fabric and 160 Mpps offorwarding rate.
2.2	Switch shall have minimum 16 K MAC Addresses.
2.3	Switch shall have minimum 1K Active VLANs.

2.4	Switch shall support minimum 1K IPv4 and IPv6 unicast routes.
2.5	Switch shall support minimum 1K IPv4 and IPv6 multicast groups.
2.6	Switch shall support minimum 1000 IPv4 and IPv6 QoS and Security ACLs.
2.7	Switch must have atleast 2GB DRAM and 2 GB Flash memory
3	**IEEE Standards**
3.1	Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w,802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.
4	**Quality of Service (QoS) requirements**
4.1	Switch shall have 802.1p class of service, IP differentiated service codepoint (DSCP) and cross stack QoS or should support QOS
4.2	Switch shall have committed information rate, rate limiting and flow-based ratelimiting.
4.3	Switch shall have minimum 8 egress queues per port and strict priority queuing.
5	**System Management and Administration**
5.1	Switch should support SSHv2, SNMPv2c, SNMPv3, NTPv3 and NTPv4.
5.2	Switch should support AAA using RADIUS and TACACS+.
5.3	Switch should support port security, DHCP snooping, Dynamic ARP inspection, IP Source guard, BPDU Guard, Spanning tree root guard and IPv6 First Hop Security ▌IPV6 access security
5.4	Switch should support software upgrades via TFTP or FTP.
5.5	Switch should support IPv4 and IPv6 ACLs, VLAN , Port and Time based accesslist with time ranges.
5.6	Switch shall have Switch Port Analyzer (SPAN) and Remote Switch PortAnalyzer (RSPAN) .
5.7	Switch shall have Layer 2/Layer 3 trace route for ease of troubleshootingby identifying the physical path that a packet takes from source to destination.
5.8	Switch shall have Internet Group Management Protocol (IGMP) Snooping forIPv4 and IPv6, MLD v1 and v2 Snooping and Multicast VLAN Registration protocol.
5.9	Switch shall have per port broadcast, multicast and unicast storm control.
5.1	Switch shall have Unidirectional Link Detection Protocol (UDLD), Link Aggregation Control Protocol (LACP), and Dynamic Trunking Protocol (DTP) or equivalent or 802.1Q
5.11	Switch should be Software Defined Networking Ready with Open flow orsimilar protocol support or Netconf

6	Regulatory Compliance
6.1	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950Standards for Safety requirements of Information Technology Equipment.
6.2	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE ClassA/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.

Blade Server

SN	Parameter	Description
1	Processors	Each blade shall have two numbers of latest Intel Xeon Scalable Processors (Intel® Xeon® Scalablefamily or higher) with Min. 24 cores per processor each having Min. 2.4 GHz processor speed.
		Processor should be latest series and generation across all the server models available.
2	Chipset	OEM compatible Chipset
3	Memory	Should be populated with 256 GB with 2933MHz DDR4 ECC Memory upgradable to 2TB Min.
4	DIMM Slots	Min 24 DIMM Slots or higher
5	Network	The server should provide interface of minimum 2* 25 Gbps ports
6	Hard Disk	Two numbers of minimum 480 GB SSD drives or higher capacity
7	RAID controller	SSD drives compatible RAID Controller to enableRAID 1, 0
8	Redundancy	The blade server to be provided with port level or cardlevel redundancy for I/O connectivity.
9	Form Factor	Half Height/ Width Blade
10	Virtualisation	Heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu, CentOS).
11	Management	The offered Management software should be capableof policy-based management using service profiles and templates.
		OEM software for management of Servers must be included as standard. Supply should include Remote Management capabilities with relevant licenses.

		The management software should participate inserver provisioning, device discovery, inventory,diagnostics, monitoring, fault detection, TPM, auditing, and statistics collection. System should support RESTful / XML API integration
12	Industry Standard Compliance	ACPI, PCIe 3.0, USB 3.0,
13	Operating Systems and Virtualization Software Support	Windows Server, VMware ESXi, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), CentOS.
		Support for either of 64bit Linux//Windows Operating System with cluster support
14	Others	The Blade should be hot pluggable
15	OEM Comprehensive warranty	5 Years Support. No additional cost for any service orparts replacement.

Blade Chassis

Sr.No.	Item	Specification
1	Enclosure	Blade chassis shall be 19" rack mountable
		The enclosure Should support full height/width and half height/width blades in the same enclosure, it should support minimum 8 half height/width blades per blade chassis
2	Power	The enclosure should be populated fully with power supplies of the highest capacity & should be energy efficient. Administrators should have the ability to set a cap on the maximum power that the chassis can drawin order to limit power consumption for non-critical applications
		The power subsystem should support N + N / N+1 power redundancy (where N is greater than 1) for a fully populated chassis
3	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers

4	Blade Support	Chassis should support Intel Scalable processors based2 CPU / 4 CPU server. Should support built-in/External management software in redundancy
		Should provide single management console for all the blade servers across multiple chassis.
5	Chassis connectivity	The chassis should provide redundant switch modulesfor proposed I/O connectivity.
	Converged Module	Chassis should have sufficient number of redundant converged modules to provide a minimum FCoE uplink bandwidth of 50 Gbps per blade server and 25 Gbps sustained Ethernet per blade server (with 1 module failure) for a fully populated chassis for converged Traffic.
		Required Network and management modules should be populated from day 1 to ensure redundancy

DDoS

Sl.no	Specifications
	DDoS Solution
	OEM ELIGIBILITY CRITERIA
1	OEM should have TAC based in INDIA
2	The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).
3	OEM Should have DDoS Scrubbing Centre in INDIA
5	OEM must have atleast 5 DDoS successful implementations in Indian Government / PSU / Defense / BFSI in last 3 years. PO Copies / Completion Certificate to be provided.
	Technical Specifications
1	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Device) with 20 Gbps of Mitigation Throughput.
2	Support Flood Attack Prevention Rate: upto 25 MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day-1 and scalable upto 10Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 1G ports, 6 x 10 GbE SFP+ from day-1 and additional 12 x 1G/10G SFP+ for future use(Without use of Breakout Cables) Latency should be less than 60 microseconds.

	The appliance should have dedicated Out-of-band Management Port.
3	System should support horizontal and vertical port scanning behavioral protection.
4	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against IoT Botnet threats at L3-7.
5	System should have DNS Flood protection for each type of query including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc.
6	System should support DNS Challenge and DNS Rate Limit.
7	System should support HTTP Challenge Response authentication without Scripts
8	System should have SIP Flood Protection, UDP and UDP Fragmented Flood.
9	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should have String Match Engine to support 1000+ Signatures from Day 1.
10	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should transparent to L2TP, GRE, IP in IP traffic.
11	The Solution should be able to synchronizes policies, baselines traffic and attack footprint between devices & Scrubbing Center (in case of future requirement).
12	The Proposed Solution should protect against Zero Day DDoS Attacks. ZERO DAY ATTACK PROTECTION should be provided using behaviour based technology.
13	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism where WAF efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter. WAF and DDoS should be from same OEM.
14	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. DNS Protections.. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Anti-Scanning Profile.
15	System should protect from DDoS attacks behind a CDN Network.
16	**The proposed Device should use the following Block Actions :** 1) Drop packet, 2) Reset (source, destination, both), 3) Suspend (source IP address, source port, destination IP address, destination port or any combination), 4) Challenge-Response for TCP, HTTP and DNS suspicious traffic

17	The proposed solution should Support REAL-TIME attacker intelligence feeds, pertaining to a active attack sources recently involved in attacks. The feed should support real-time and ongoing validated and actionable threat intelligence from multiple sources for preemptive protection.
18	OEM should Support 24x7 (SLA defined), REAL TIME Emergency Response Services for the network facing denial-of-service (DoS) attack in order to restore network and service operational status.
19	For future Scalability, The proposed solution should support Integration with OEM Cloud based Scrubbing Centers, in case of Bandwidth Saturation attacks, using the same technology.
20	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1.

Network Intrusion Prevention System (NIPS)

- The NIPS solution should be comprehensive of hardware, software, licenses, etc.

- IPS solution should have 10 Gbps of real-world throughput with scalability up to 40 Gbps on same appliance or through stacking
- Should be a standalone independent hardware-based NIPS appliance and should be other than Router, Internet Firewall, Intranet Firewall, DDoS and Load balancer based vendors to avoid any single point of failure.
- Should support VA scanners (Qualys, Rapid 7, and Nessus) to fine tune the IPS policy automatically
- Intrusion Prevention System (IPS) should be based on purpose-built platformthat has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch anddual plane architecture for Data and control plane and NIPS should be independent standalone solution

- The proposed IPS must able to operate in Asymmetric traffic environment with signatures/Filters protection

- The proposed IPS solution must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption and memory errors
- Should intercept and inspect 8 Gbps SSL traffic for any malicious content without performance degradation
- 20 million legitimate concurrent Sessions/Connections scalable upto 100 million and 70000 new Connections per second scalable up to 650,000. Scalability can be achieved using single or multiple appliances leveragingstacking functionality.
- The proposed IPS must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLANtraffic in the same way as in-line deployment

- The OEM of the proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant report for Intrusion Prevention Systems in each of thelatest last two reports
- Should be able to manage locally independently without any centralized management server
- Latency <40 microseconds and information should be publicly available and documented
- Should protect all Inter-VLAN traffic in the same way as in-line deployment.
- Support firmware, signature upgrade/Reboot without require downtime
- The proposed IPS must have the capability to convert other vendor's signature(such as snort)
- Should bypass traffic for IPS internal issues i.e. memory hang, firmware crashetc.
- IPS must provide bandwidth rate limit to control the unwanted traffic such asP2P, Online Game, etc.
- IPS must have a power failure bypass modular that can support hot swappablefunction which allows traffic to bypass even after a modular get unplugged out of IPS Box during the RMA procedure
- The proposed IPS solution must support Adaptive Filter Configuration (AFC)which will alert or disable ineffective filter in case of noisy filters
- The proposed management system shall support 'threat insights' dashboardthat show correlated data such as how many breached host, how many IOCdata, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered
- The proposed IPS must be able to support GTP inspection for GPRS/3Gmobile networks
- ☐ The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin

- The proposed management system shall also be able to provide a customized'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through
- The proposed IPS system must support SNMP and a private MIB that can beutilized from an Enterprise Management Application such as HP Openview, MRTG, etc.
- The central management server should serve as a central point for IPS security policies management including versioning, rollback, import and export (backup) tasks.
- The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abusereport, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report
- Should supports inspection of Asymmetric traffic consisting jumbo frames,DGA Defense filters, Machine learning, Virtual patching capability.
- Should have ransomware filters utilize a "trace" action set to extract a private key from the network flow in order to help restore encrypted files to the victim while blocking traffic to the CnC server

- Should have real-time Portal which gives security posture of the internet, helping customers to know more information about signatures and threatsassociates with it.
- Should Integrates with Qualys, Tenable, Rapid7 for importing vulnerabilitiesand creating profile.
- Should have dedicated Management Appliance having hardware based securestorage for sensitive data (PKI management/SSL)
- Should have Vulnerability based filters covering entire Vulnerability footprint, which understands various exploit patterns.
- Should have zero downtime during RMA, Rate limit on non-business traffic i.e.bit torrent and Big data engine in management platform for faster report generation
- Should be based on purpose-built platform that has Field Programmable GateArrays (FPGAs), CPU's, On-board L2 Switch and dual plane architecture for Data and Control plane.
- Should bypass traffic for IPS internal issues i.e. memory hang, firmware crash even with the power on, in event of un-recoverable internal software error suchas firmware corruption and memory errors
- Export network flow data statistics to optimize performance and help identify compromised hosts and other suspicious and malicious network traffic.
- The management server must support the archiving and backup of events andexport to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.

- The proposed IPS should integrate with on premise sandbox (APT solution) as per RFP specification to submit unknown samples for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to NIPS toblock threats.
- Should have at least inbuilt 15000 signatures/Filters pertaining to security and applications apart from user define signatures/filters
- Proposed solution should not be declared end of sale and end of support forcoming 5 years.
- Proposed solution should natively integrate with on – Premise sandbox solutionto detect and mitigate zero day threats having common threat sharing management platform.

Support

- OEM Support should be available 24*7 through email and telephone at no additionalcost and should be part of annual maintenance
- Should have a support centre
- Should provide Five year support from the date of Go-Live of SDC for completeNIPS including update, upgrade, licenses, patches etc.

Physical Requirements

- o 19" Rack Mountable

- o All necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, wire managers, etc. should be provided to install NIPS in the Data Centre

2.1.2 Server Load Balancer

Sl.no	Specifications	Compliance (Yes/No)
	SLB	
	OEM ELIGIBILITY CRITERIA	
1	OEM should have OEM TAC in INDIA.	
2	OEM should have atleast 5 References in the Government / BFSI / Defense in the Last 3 Years for the proposed Technology.	
3	The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).	
	Technical Requirement	
1	**Traffic Ports support :** 2 x 10 GE, 8 x 1 GE RJ45 (**without use of Breakout Cable**) **Device L4 Throughput** : 5 Gbps and scalable upto 25 Gbps (Dedicated WAF Throughput : 3 Gbps) **Layer 4 connections per second :** 500K CPS **Layer 7 requests per second :** 700K RPS **SSL Throughput :** 10 Gbps **Concurrent Connection**: 20 Million	
2	The proposed Appliance should be equipped with minimum Intel Quad-core CPU. SLB & WAF Should be from same OEM in the proposed appliance.	
3	The Proposed Device should support ICSA certified Web Application Firewall. The Proposed Appliance should have Below features from Day 1: 1. Advance Web Application Firewall License. 2. Regular Automatic WAF Signature Updates as part of OEM's own intelligence feed.	

4	**VIRTUALIZATION:** The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware, KVM etc.). **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 5 Virtual Instance from Day 1 and support upto 20 Virtual Instances for future Scalability on the same hardware. It should NOT use Open Source/3rd party Network Functions.	
5	The Proposed Appliance should support Standalone as well as Virtualized Mode from Day 1 (Bidder may be asked to demonstrate this feature during Technical Evaluation).	
6	The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (no proprietary protocol).	
7	The Proposed Device should NOT have Open Source/3rd party Hypervisor/Network Functions.	
8	Device should be accessed through the below: • Using the CLI • Using SNMP • REST API • Using the Web Based Management	
	Server Load balancing	
9	**The proposed appliance should support the below metrics:** — Minimum Misses, — Hash, — Persistent Hash, — Tunable Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc	

10	**Following Server Load Balancing Topologies should be supported:** • Virtual Matrix Architecture/Equivalent • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding	
11	A framework for customizing application delivery should be provided using user-written scripts, that provides the flexibility to control application flows and fully meet business requirements in a fast and agile manner. **The proposed framework should enables to:** • Extend Server Load Balancer Fabric services with delivery of new applications • Quickly deploy new services • Mitigate application problems without changing the application • Preserve infrastructure investment by adding new capabilities without additional equipment investment	
12	Device must support static and dynamic routing protocols like OSPF, RIP1, RIP2, BGP, etc. from Day 1.	
13	DNSSEC based Global Load Balancing should be supported in the proposed device from Day 1.	
14	The propsed Device should have the Proximity based LLB which monitors 24/7 Full-path transaction completion through Application-aware full-path Health Monitoring module and automatically measures the real-time status of two-way routes between the network and the remote user or servers on the internet based on multiple parameters including latency, packetloss, Cost and load time of the link.	
	Web Application Firewall	
15	The proposed Solution should have NSS Lab recommended/ ICSA Certified/ PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification	
16	WAF OEM Should be different from Network Firewall OEM.	
17	Proposed WAF should have the flexibility to be deployed in the folowing modes: Reverse proxy Out of Path (OOP)	
18	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter. WAF, DDOS and ADC should be from same OEM.	
19	WAF Should support both Negative & Positive Security for Zero-Day protection.	

20	The WAF should support the following escalation modes:
	    a) Active,
	    b) Bypass,
	    c) Passive	

21	**Hiding Sensitive Content Parameters:** It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)	
22	**WAF should support for IPv4 and IPv6 traffic**	
23	**Auto Policy Optimization**	
	• Known Types of Attack Protection - Rapid Mode	
	• Zero Day Attack Blocking - Extended Mode	

	• Security Filter Auto Policy Generation
	    a) Full Auto
	    b) Auto Enabled
	    c) Auto Refinements	

	• Auto Discovery	
24	**Following Threats should be protected by the proposed WAF solution:** Parameters Tampering Cookie Poisoning SQL Injection Session Hijacking Web Services Manipulation Stealth Commands Debug Options Backdoor Manipulation of IT Infrastructure Vulnerabilities 3rd Party Misconfiguration Buffer Overflow Attacks Data Encoding Protocol Piggyback Cross-Site Scripting (XSS) Brute Force Attacks OS Command Injection Cross Site Request Forgery (CSRF) Hot Link Information Leakage Path (directory) Traversal Predefined resource location Malicious file upload Directory Listing Parameter Pollution (HPP)	
	Device Fingerprint-based tracking	

26	The Proposed WAF should support Device Fingerprint technology or equivalent by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc. It should support running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to the WAF with the fingerprint information.	
	Integrated Bot Management Solution support	
27	The proposed Solution should support Bot Management functionality or equivalent that provides comprehensive protection of web applications, mobile apps and APIs from automated threats like bots by combining behavioral modeling for granular intent analysis, collective bot intelligence and fingerprinting of browsers, devices and machines.	
28	It should support protection against all forms of account takeover (such as credential stuffing and brute force), denial of inventory, DDoS, ad and payment fraud, and web scraping.	
29	It should support customized response using : 1. Allow 2. CAPTCHA 3. Block 4. Fake Feed.	
	Centalized Management	
30	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1. Proposed SLB, WAF, and DDoS should be Managed from the Same Centralized Management Solution.	

2.1.3 Virtualisation and unified management

Sr. No	Specifications
1	The solution should include bare metal hypervisor with centralized management platform for managing virtual infrastructure including functionality of High Availability,near Zero Downtime & near Zero Data-loss , Encrypted Live Migration of VMs across DC & DR, Hot Add (vCPU, vMemory, vStorage & vNIC) without any disruption of VMs, Distributed Switch with latency sensitivity and link aggregation, enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN, Network and Storage I/O Control, , dynamic resource schedulingfor storage and VMs, SR-IOV and secure the VMs with offloaded AV/AM solutions without the need for agents inside the virtual machines.

2	The solution should provide proactive High availability capability that utilizes serverhealth information and migrates VMs from degraded hosts before problem occurs and secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.
3	The solution should have single reboot to dramatically reduce the upgrade times byskipping a host reset and also help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time-consuming hardware initialization
4	The solution should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.
5	The solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into proactive monitoring, alerts, management, capacity planning, performance management, reclaim resources, infrastructure behaviour, upcoming problems, root cause analysis, what-if scenarios, and opportunities for efficiency improvements.
6	The solution should provide Self-service Provisioning portal for end-user with Approval governance, deployment cost and admin portal with drag and drop feature
	for cloud agnostic blueprint design.
7	The solution must have Resource Reclamation, Rightsizing, Capacity planning, Configuration, Compliance and Customizable Dashboards and Reports.
8	All the software components should have support for 24x7x365 with updates andupgrades during the complete tenure of the project.

Advance Persistence Threat Solution (Anti - APT)

1. Solution must be a custom built on premise Anti-APT solution and must not from UTM andNGFW vendors and should not be a CPU and chip based function.
2. The proposed solution should support to monitor traffic from multiple segments.
3. The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.
4. The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, WindowsRegistry entries, File hashes, Malware detections through a dashboard
5. The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable.
6. The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IPAddress of a host in a proxy/NAT environment.
7. The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols forinspection.

8. The proposed solution should have a built-in document vulnerabilities detection engine toassure analysis precision and analysis efficiency.
9. The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session.
10. The proposed solution should have an endpoint security component with following functionalities (Antivirus, Vulnerability Protection, Data loss, Application control, EDR andMDR with ability to automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.
11. The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox.
12. Solution should be deployed on premise along with on premise sandboxing capability andno data should be allowed to go on public cloud.
13. The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.
14. Proposed solution should be able to provide customizable sandbox to match customer'sendpoint environments
15. The solution should allow administrator to categorize files as safe based on Hash values(MD5) and should record network metadata retroactively & play out entire attack event

    with click of a button to see attack lifecycle chronologically including URL redirects, initialinfection point and lateral spread.
16. The proposed solution should support to monitor traffic from multiple segments like WAN,DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
17. Proposed solution should have 2 TB in RAID 1 of on box storage from day one with a scalability of 8 TB
18. The proposed solution should be able to run at least 20 parallel sandboxes imagesscalable up to 60 for analysis of payload
19. Customized sandbox solution should support following operating systems (Windows XP,Win7, Win8/8.1, Win 10, Windows Server 2008, 2012, 2016 and CentOS)
20. Solution shall be capable to hold a downloading file while it is first seen in the network andis heuristic that needs to be analyzing by sandboxing. While in the holding, the solution shall be capable to return end-user a notification page. The solution should block the file after the analysis of sandboxing in case the risk of suspicious file is high and the file type shall be supported as minimum requirement are: Windows PE files, Archive file type (Zip, tar), All Microsoft Office file type, Adobe Acrobat PDF, PowerShell
21. The destination website in both intranet (in corporation network) and internet (typical internet website) shall be supported as patient zero functionality
22. Solution shall be capable to decrypt the traffic and perform all content/payload scanning for APT preventions. Solution shall be capable to automatically bypass the traffic to avoidthe broken connections while solution is trying to decrypt the traffic.
23. Solution shall be capable to intercept, decrypt, content inspections for advanced persistent threats consisting HTTP 1.1, HTTP 2.0 (HTTP/2), HTTP with TLS, Up to TLS 1.3 version protocols
24. Solution shall be capable to perform threats inspection over 40,000 con-current HTTPSsessions
25. Forward proxy mode - Under this deployment mode, Solution shall be capable hosted aseither a standalone proxy or proxy-chaining with other web proxy and under the proxy- chaining mode, Solution shall be capable to read XFF(X-Forwarder-For) header for logs and policy making while it is working as upstream proxy.
26. Transparent high availability mode - Under this deployment mode, Link Aggregation Control Protocol (LACP) is available to aggregate two network interface cards to form a single logical link

(link aggregation group) and Under this deployment mode, Solution shallbe capable of processing web traffic that is routed through redundant network configuration

27. Solution must support Custom Sandbox Domain Check, Software Check, User Settingscheck, perquisite file check, Office version check, Windows License check, Browser Check (Sandbox Customized with OS and Applications in the Environment to maximizetargeted attack detection capabilities)
28. The Proposed Solution should support End-User Quarantine feature
29. Solution should be able to centrally manage and deploy sandbox image update tomanaged products.
30. Solution should be able to centrally manage and deploy product updates includingpatches, hotfixes, and firmware upgrade
31. The proposed solution should have bi - directional seamless integration with Endpoint Security, HIPS and NIPS for detecting and mitigating zero day threats leveraging sandboxanalysis.

Perimeter/external Firewall

Feature	Technical Specification	Compliance Y/N
Hardware Architecture	The appliance-based security platform should provide firewall, IPS, URL filtering, AVC and AMP functionality in a single appliance from day one	
	The appliance should support atleast 8*10G Gigabit ports and 4 * 40G from day one including Transceivers.	
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory	
	Proposed Firewall architecture based on multi-core cpu's to protect & scale against dynamic latest security threats	
Performance & Scalability	Should support 10 Gbps of NGFW (FW, AVC, and IPS) real-world / production performance from day one	
	Firewall should support at-least 20,000,000 concurrent sessions	
	Firewall should support at-least 400,000 connections per second	
	Firewall should have integrated redundant hot-swappable power supply	
	Firewall should have integrated redundant fan	
	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc	

Firewall Features	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	Should support Multicast protocols like IGMP, PIM, etc	
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance	
	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency	
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Should support more than 11,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports	

	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events	
	Should be capable of detecting and blocking IPv6 attacks	

	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor repuration of IP addresses determined by the proposed security vendor	
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	Should must support DNS threat intelligence feeds to protect against threats	
	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.	
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	

	Should support customized Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
URL Filtering Features	Should must support URL threat intelligence feeds to protect against threats	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 70 categories.	
	Should support troubleshooting techniques like Packet capture	
	Should support REST API for monitoring and config programmability	
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
	Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one	
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	The management platform support running on-demand and scheduled reports	
	The management platform must risk reports like advanced malware, attacks and network	
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools	

Support	Proposed solution should support 24x7x365 OEM TAC support	

2.1.4   Database Server

S.No	Item	Specification for Rack Based Servers
2	Processors	Rack Server shall have a minimum of two (2) scalable to four (4) Intel latest generation Xeon Scalable Processors (Launched in 2021) / AMDEPYC (Launched in 2021) with minimum 2.6 GHz and 24 MB Cache & minimum 16 cores per socket. Or Rack Server shall have a minimum of One (1) scalable to two (2) Intel latest generation Xeon Scalable Processors (Launched in 2021)/ AMDEPYC (Launched in 2021) with minimum 2.6 GHz and 48 MB Cache & minimum 32 cores per socket.
3	Chipset	Intel chipset compatible with the offered processors.
4	Internal Storage	The server should Support upto 8 hot-swappable SAS and SSD drives.
5		Server should be configured with 4 Nos 1.6 TB SSD drives, the server be proposed with 2* 480 GB M.2 SSD boot drive with HW RAID Controller
6		
7		Server should be configured minimum with 4GB of Flash backed writecache module.
8	Memory	Should have at least 24 DIMM slots per server and the server should beconfigured with 1.5 TB DDR4 Memory from day one
9		
10		Support for advanced memory redundant technologies like Advancederror-correcting code (ECC)
11	Network	Should have 2 * 10 GbE (embedded) LAN ports, 4*25 GbE network portsfor LAN connectivity (in case only one processor is populated, 2*25 GbE network ports shall be provided from day 1 and shall be scaled to 4*25 GbE ports at no extra cost to client when the second processor socket is populated)
13	PCIe Slots	Up to 6 PCIe Generation 3.0 slots. In case only one processor is proposed, Up to 3 PCIe Generation 3.0 slots (and Up to 6 PCIe Generation 3.0 slots at no extra cost to client once both processor sockets are populated)
14		2 x dual port 16 Gbps Fiber Channel HBA
28	Ports	Should have the following ports for server connectivity
29		● 1 serial port
30		● 3 USB 3.0/2.0 ports
31		● 1 VGA video port
32	Others	Supports hot swappable redundant fans
33		Supports hot swappable redundant power supplies
34		Rail Kit and cable management arm to be provided along with the server

36	Form Factor	2U Minimum
37	Compatibility	Proposed Rack servers should be compatible and shall connect witheither existing fabric interconnect switch ==or with new Access Switch proposed.==

Antivirus Software

Latest Antivirus Software with update and upgrade for a period of five years with following features:

1. The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection
2. Endpoint solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, EDR, DLP, XDR and MDR capabilities in a single agent
3. Proposed solution should have Pre, Post and Runtime machine learning capability
4. Proposed solution should have True file type scan along with Proactive outbreak prevention and Command & Control callback detection
5. File reputation - Variant protection - Census check - Web reputation
6. Advanced malware and ransomware protection: Defends endpoints—on or off the corporate network—against malware, Trojans, worms, spyware, ransomware, and adaptsto protect against new unknown variants and advanced threats like crypto malware and fileless malware.
7. Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability
8. Behavior monitoring along with ransom ware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same.
9. Proposed solution should have IPv4 and IPv6 support
10. Endpoint solution should have data loss prevention with pre-defined templates for HIPAA,PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based
11. Offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP.
12. Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).
13. Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network
14. Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity ofthe application
15. Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting.
16. Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates).
17. Ensures that patches/updates associated with whitelisted applications can be installed, aswell as allowing your update programs to install new patches/updates, with trusted sources of change.
18. Features roll-your-own application whitelisting and blacklisting for in-house and unlisted applications.
19. Limits application usage to a specific list of applications supported by data loss prevention(DLP)

products for specific users or endpoints.
20. Collects and limits application usage for software licensing compliance.
21. Proposed solution should not send any file/sample with cloud to inspect and analyze forany threat
22. Features system lockdown to harden end-user systems by preventing new applicationsfrom being executed
23. Should be capable of recommending rules based on vulnerabilities on endpoint andcreate dynamic rules automatically based on System posture and endpoint posture
24. Blocks known and unknown vulnerability exploits before patches are deployed
25. Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable
26. Automatically assesses and recommends required virtual patches for your specific environment.
27. Dynamically adjusts security configuration based on the location of an endpoint.
28. Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and commandand control (C&C) blocking.
29. Provides protection before patches are deployed and often before patches are available
30. Shields operating system and common applications from known and unknown attacks
31. Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information
32. Scans and remediates compressed archives for malware without requiring unnecessary decompression
33. Safeguards a wide range of network attached storage systems by detecting and removingviruses and spyware in real time
34. Comprehensive storage security uses the industry-standard ICAP protocol to complementsupport for traditional RPC communication protocols
35. Should protect storage devices i.e. EMC, NetApp, Hitachi Data Systems storage systemsetc.
36. Solution must support CPU usage performance control during scanning -Checks the CPUusage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.
37. Solution should encrypt private data with fully integrated full disk, file folder, USB, and removable media encryption
38. Should manage encryption policies and protect data on PCs, Macs, laptops, desktops,USBs, and removable media
39. Should have common management console to manage both Endpoint AV and Encryptionfor better visibility and control.
40. Should be capable of Powerful Investigative Capabilities (EDR) including :
41. Investigation and IOC Sweeping (server-side metadata sweep)
42. Patient Zero ID / Root Cause Analysis and IOA Behavior Hunting/Detection
43. API's for query / automation and Unknown file guidance
44. Variant Protection to detects mutations of malicious samples by recognizing known fragments of malware code
45. Packer Detection to Identifies packed malware in memory as it unpacks, prior to execution
46. Runtime Machine Learning scores real-time behavior against a cloud model to detect previously unknown threats

47. IOA Behavioral Analysis detects behavior that matches known indicators of attack (IOA), including ransomware encryption behaviors, script launching
48. In-memory runtime analysis malicious script detection, malicious code injection, runtimeun-pack detection
49. Isolation, Quarantine, Process kill, Execution block and Damage rollback
50. Provides context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess thenature and extent of an attack. Custom detection, intelligence, and controls
51. Record detailed system-level activities and perform multi-level search across endpointsusing rich-search criteria such as OpenIOC, Yara, and suspicious objects.
52. Detect and analyze advanced threat indicators such as fileless attacks.
53. Root cause analysis for simple or full "kill chain
54. Search by multiple parameters by OpenIOC rule for disk scans and Yara rules for memoryscans
55. Solution should be APT ready capable of submitting SO (Suspicious Objects) to On-Premise Sandbox appliance for analysis without additional License on Endpoint.
56. Integrates with other security products locally on network and also to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enablingfaster time-to-protection and reducing the spread of malware
57. Solution should have capability to submit unknown files to On-Premise sandbox appliancefor simulation and create IOC's on real time basis as per sandboxing analysis and revert back to Endpoint security solution.
58. Should have seamless integration with Anti – APT solution bi-directionally to detect and mitigate zero day threats having common threat sharing platform for holistic visibility and control.

Security Incident Management Solution

S. No.	Description	Complied Y/N
1	Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deeppacket inspection high speed packet capture and analysis.	
2	The solution should be able to collect raw logs in real-time to a Central logdatabase from any IP Device including:	
	Networking devices (router/switches/voice gateways)	
	Security devices (IDS/IPS, AV, Patch Mgmt, Firewall/DB Security solutions)	
	Operating systems (Windows 2008/2012/16/19/Linux)	
	Virtualization Platforms (Microsoft HyperV, VMware Vcenter/ VSphere 4.X)	
	Databases (Oracle/SQL/MYSQL/DB2)	

3	The solution should have following components:	
	a. Management & Reporting	
	b. Normalization and Indexing	
	c. Correlation Engine	

	d. Data Management	
4	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP and Encryption,application security	
5	The solution should be able to collect the logs in an agent/ agent less manner and store the same in real-time to a Central log database from any IP Device. The logs should be time stamped, compressed to optimize storage utilization. There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.	
6	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle.	
7	The solution should collect the entire log sent by the devices. This will help in maintaining digital chain of custody. These logs can be modified by a malicious indented user. In order to make these logs tamper proof solution must store events in compressed archives that are temper proof encoded. Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlationrule processing. In addition solution must provide contextual Hub at investigationlayer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc	
8	The solution should provide tools for developing collection and parsing capabilities for home-grown or any other unsupported /unknown IP applications.The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.	
9	The system should provide for integration with third party ticketing systems forescalated incidents that need escalation.	
10	The tool should provide flexible dashboard interface customized to user preferences allowing the examination of a specific event or a holistic view of thesystems within the enterprise. Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration	
11	The tool should have the capability to fetch logs from the solution in real time ordesired period (hours/days/specific period etc) to ensure comprehensive trend and historical analysis and reporting.	
12	The solution should allow filtering log data based on log message payload like source and destination IP, ports, usernames, workstation address, domain etc.	
13	The Solution must provide remediation of the incidents by prioritizing incidents based upon the security policies and generating tickets for a quick response to security threats associated with the affected assets. It should also be track thesechanges.	
14	Solution should support minimum 30,000 EPS scalable to 50,000 at correlation,management and collection layer and packet capture solution should support	
	upto 1GBPS line rate for capturing from network.	

15	The solution should be storing both raw logs as well as normalized logs. Should store RAW packet DATA for 7 days and normalized packet data for 120 days forforensics.	
16	All necessary dedicated hardware (with min 12TB storage in raid 5/6) forSecurity Incident Management Solution should be provided.	

2.1.5 SAN Storage

S. No.	Minimum Requirements	Complied (Y/N)
Make / Model:		
1.	Data Availability 1. Offered storage shall be an Enterprise Storage array shall provide 99.999% or more data availability. 2. Documentation for 99.999% availability shall be submitted along with bid.	
2.	Offered Storage shall be supplied with at-least Dual controller with scalability by adding new controllers, true symmetric/ asymmetric active-active controller while supporting all the major functionalities like Thin Provisioning, RAID Parity calculations etc.	
3.	Offered Storage system should provide minimum 200000 IOPS with 70:30 Read/write ratio and 8K block size along with data efficiency feature enabled from day one. Bidder has to provide sizing tool output of OEM along with tender document.	
4.	Offered Storage array should have at-least 192 GB Data Cache and shall be scalable to at-least 512 GB Data Cache. It shall support de-staging of cache to disks on power down or shall support internal battery backup of cache for at least 72 hours. The data in cache shall not be lost in the case of power failure.	
5.	Storage should support for SSD, SAS along with NL-SAS / MDL-SAS disks with a scalability to min 500 Disks	
6.	It should support hardware RAID levels 6 or better.	

7.	The storage must be configured with minimum 320 TB usable Capacity in RAID 6. With the following Disk configuration - 30% Flash/SSD, 30% SAS, 40% NL SAS. SSD, SAS and NL SAS should be in RAID 6 Vendor shall use OEM best practices while sizing the array. Best practices documentation to be submitted by OEM to validate the sizing.	
8.	Offered Storage array shall have minimum of 16 x 32Gbps Fiber Channel ports 8 x 25Gbps/10 Gbps ISCSI ports. All ports shall have capability to work at line speed. Offered Storage should have minimum 384 Gbps SAS/FC backend scalable to 576 Gbps	
9.	Offered Storage should support either thin reclaim natively or bidder need to provide solution for thin reclaim	
10.	It should support heterogeneous client OSs, which includes all popular flavours of Windows, Unix and Linux along with Virtualisation Softwares like Vmware etc.	
11.	Dedicated management ports needs to be provided in additional to the host ports required above	
12.	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc. The same should support minimum 2000 LUNs/ Initiators	
13.	The storage must have the capability to expand LUNs/volumes online. Offered storage shall support dynamic migration of Volume from one RAID set/pool to another set/pool while keeping the application online	
14.	1. The storage array should have support for controller-based snapshots (At-least 254 copies for a given volume). 2. Offered Storage array shall support more than 20000 base volume on the storage array without snapshot and clone.	

15.	The storage should be configured with Thin provisioning and thin reclaim natively or bidder need to provide solution for thin reclaim.	
16.	Must support replication features (Synchronous and Asynchronous) for block data. Must support three site replication features natively/ with additional hardware. DC to DR Async and DC to Local HA / Near DR Sync replication is envisaged	
17.	Comprehensive management software for fully managing and administering the storage including deployment, automation, provisioning and monitoring	
18.	All necessary cables for enclosure interconnections must be part of the storage system supply	
19.	Storage subsystem shall be supplied with Thin provisioning, Snapshot, Clone, Performance Monitoring, Quality of services, for the maximum supported capacity of array.	
20.	Offered storage array shall be true multi-tenant and shall support more than 240 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.	

2.1.6   SAN Switch

S. N.	Minimum Requirement	Complied (Y/N)
Make / Model:		
1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'	
2	The switch to be configured with minimum of 128 ports scalable to 176 ports with 16 Gbps FC configuration backward compatible to 4/8.	
3	All 128 x FC ports for device connectivity should be 4/8/16 Gbps auto- sensing Fibre Channel ports	

4	The switch must have hot-swappable redundant control plane module/supervisor, fabric modules, power supply & fan module without resetting the switch, or affecting the operations of the switch	
5	The switch must be able to support non-disruptive software upgrade	
6	The switch must be able to support state full process restart	
7	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience	
8	The switch must support up to 8 Virtual Fabric Instances	
9	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances	
10	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances	
11	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers	
12	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning	
13	The switch must support Smart Zoning such that the entries in TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric	
14	The switch must support Power On Auto Provisioning (POAP) and Quick Configuration Wizard for simplified operations	
15	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics	
16	The switch must support routing between Virtual Fabric instances in hardware	

17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication	
18	ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported	
19	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link	
20	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches	
21	The switch should support IPv6	

2.1.7   Tape Library

S. No.	Minimum Specification	Complied (Yes / No)
Make / Model:		
1.	Shall support Native data capacity of ~~200~~ 576 TB (uncompressed) expandable to ~~400~~ 1152 TB (compressed)	
2.	Shall be offered with Minimum of four LTO8 and 1 LTO7 FC tape drive. Drives shall support encryption	
3.	Shall be offered with minimum of 48 Cartridge slots and scalable to minimum 100 Cartridge	
4.	Tape Library should be backward compatible and ~~some (10%) Cartridge slots~~ 1 tape drive should support min LTO 6	
5.	Tape Library shall provide 8Gbps/ 16 Gbps native FC connectivity to SAN switches	
6.	Library shall be able to back up the encrypted keys in a redundant fashion using Industry standards like Application Managed Encryption (AME) or Library Managed Encryption (LME) or Centralized Encryption Key Manager Appliance	
7.	Tape Library shall provide web based remote Management	

8.	The library should have cartridge I/O slots for secure & easy off-site backup storage	
9.	✓ Tape Library shall have GUI Panel ✓ Shall be rack mountable ✓ Shall have option for redundant power supply	
10.	Should support industry leading backup software	
11.	All required items like cables and HBAs should be supplied. The vendor should provide all necessary components, such as cables, adapters, to connect the tape library to the proposed storage/server/SAN switches.	

2.1.8   Backup Solution

	Specifications:	**Compliance Y/N**
1	The proposed backup solution should be available on various OS platforms such as Windows, Linux and UNIX platforms.	
2	The proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration	
3	The proposed backup solution should allow creating tape clone facility after the backup process.	
4	The proposed backup solution shall be configured in such a fashion that no extra license for client and media servers is required while moving from LAN to SAN based backup	
5	The proposed backup solution supports the capability to write up to 32 data streams.	
6	The proposed backup solution supports de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restore operation to client/servers.	
7	The proposed backup solution has inbuilt mediamanagement and supports cross platform device and media sharing in SAN environment. It provides a centralized scratched pool/auto media management thus ensuring backups never fail for media.	

8	The proposed backup solution has in-built frequency and calendar based scheduling system.	
9	The proposed backup solution has certified —hot-online backup solution for different type of enterprise databases and applications	
10	The proposed backup solution shall also support granular recovery for VMware, Exchange server	
11	The proposed backup solution must support at least AES256- bit encryption capabilities.	
12	The backup software should support priority based backup schedule, missed job execution and Advanced Scheduling option.	
13	The backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions	
14	The backup software should be capable to supporting more than 10K backup sessions in day and 1000 concurrent sessions	
15	The backup software should support the parallel backup of VMDK files	
16	The backup software should support automated replication/ synchronization	
17	The backup software should support de-duplication device like store once and data domain	
18	The backup software should have licenses to backup data to 8 SAN based tape drives with 150 slots	
19	License as per SDC requirement during the currency of contract. The backup should complete in 4 hours window.	

2.2   SDC Architecture – Physical Infrastructure

2.2.1   <u>Layout of Data Centre</u>

In the schematic below, entire SDC area is logically divided in Zones as per MIT guidelines. Each of these zones are having different objective described further in this section. Total space for SDC is 4780 sq. feet at Mehli. Total area for Server farm is 2228 sq. feet and 1326 sq. meter for NOC, BMS etc at

ground floor. Initially an area of 1014 sq ft was developed as Server Farm Area and rest of the area is earmarked for future expansion. For security purposes the entire first floor is under video surveillance and every movement is monitored, all the doors accessible to Server Farm have Biometric and Smart Card based Security. Reception Area to validate entry to the visitors by issuing guest entry passes and to keep belongings like cell phone, camera, USB drives etc. at the reception itself. Complete record of the same needs to be maintained.

For future expansion in Phase 2, the available area is approx. 1026 sqft on 1st floor in which26 racks are to be hosted and UPS room will be provided at the ground floor for installing required UPS along with batteries and electrical panels.

- **Total available area:**

S. No.	Room (Existing)	Area (in Sqft.)
1	Server Farm Area	1014
2	UPS Room	404.8
3	NOC Room	423.5
4	Staging Area	115
5	Storeroom	75
6	Project Manager Room	127.5
7	BMS Room	127.5
8	RAMP Area	59.5
9	Passage 1	122
10	Waiting Area	120
11	**Area for Expansion – 1ˢᵗ Floor**	**1026**
12	**Area for Expansion – Ground Floor**	**405**

2.2.2 Server Room

The server farm area within the SDC will host / co-locate Servers for various Departmental Application including the Database Servers. These servers may be Low end to High-end depending upon the applications hosted on them. These servers may be online or only for repository purpose. The applications, which are running on the central-computing servers, will have load balancing and high availability features.

This area will contain all the networking components from routers, switches to passive components. All the Data Center Inter-Rack connections will be provided through switches placed in this area. This area will host the Security components. The security architecture will provide controlled access to the

web and database servers from Internet and other networks. This would be multi-layer architecture with two layers of firewall separating the Internet, web, and database/application and Intranet zones.

2.2.3   UPS & Electrical Room

This area shall house all the Un-Interrupted Power Supply Units and Batteries accompanying this component. As these components generate good amount of radiation it is advised to house these components in a room separate from main SDC room.

2.2.4   Air Conditioning

Since Server Room is a critical area, a separate air conditioning system (precision air conditioning) should be exclusively installed to maintain the required temperature for Server Room. Electrical Room can have a separate air conditioning system for comfort. The general requirements for the two zones are as specified below:

- Server Room Area : should be provided with InRow Precision Air Conditioning on a 24 x 7 operating basis at least meeting with Tier-II architecture requirements and having enough provision to scale it to next level as may be required in a later stage. The units should be able to switch the air conditioneron and off automatically and alternately for effective usage. The units should be front/horizontal air-flow fashion, air-cooled conditioning system. In-Row Precision Air Conditioning systems specifically designed for stringent environmental Control with automatic monitoring and control of cooling, heating, humidification, dehumidification and air filtration function should be installed.
- UPS & Electrical Room : should be provided with split-type comfort air-cooled system (at least meeting with Tier - II architecture requirements).

Note: Bidder has to fabricate MS outdoor structure for PAC and CAC outdoor units in his scope.

2.2.5   Humidity, Ventilation and Air Conditioning Systems

Sr.	Prevision In-Row Cooling system for Data Center
1	The SDC shall be provided with fully redundant Microprocessor based Precision In- Row Cooling Units. The precision unit shall be air cooled refrigerant system with N+1 configuration.

2	Cold Aisle containment should be provided at existing and expansion area and the In-Row cooling units for SDC shall be provided with Microprocessor based PrecisionAir-conditioning system. The precision unit shall be air cooled gas based refrigerant system with N+1 configuration on low level with low power consumption. Cool air feed to the SDC shall be horizontal air flow ensuring no air stratification across the face of the IT racks. The system shall be floor mounted placed next to server racks and configured for horizontal airflow with draw-through air pattern to provide uniform air distribution over the entire face of the server racks. Positions of Indoor units shall be done wisely to reduce the distance of return air path from hot aisle to hot-air in- take of cooling units. Cooling units shall be positioned as closer to the heat load, so that any kind of recirculation of air can be avoided i.e. next to the IT racks.
3	The Bidder should work out design tonnage and air flow CFM values/ requirements for Data Centre. All the design parameters and head-load estimation calculations in detail need to be submitted for the Data Centre.
4	The bidder needs to provision and include the low side works for the augmentation ofsecond phase for future expansion in the server room.
5	**Temperature requirements**
5.1	The environment inside the SDC shall need to be continuously maintained at 22 degree $\pm$ 2 degree Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shallbe monitored on a 24x7 basis and logged for providing reports.
6	**Relative Humidity (RH) requirements**
6.1	Ambient RH levels shall need to be maintained at 50% $\pm$ 5 non-condensing. Humiditysensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.
7	**Cooling version**
7.1	The unit will feature a cooling circuit with digital/inverter compressor. This is equippedwith an electronic controller for managing cooling capacity. An electronic board fitted with microprocessor will control effective compressor capacity using a PID algorithm (proportional — integral — derivative) so as to ensure continuous and precise modulation of compressor rotation speed, R410A ecological refrigerant or equivalent. The cooling circuit will include : electronic thermostatic valve, solenoid valve, high and low pressure switches, liquid sight glass and filter-drier. The low pressure switch features automatic reset and activation can be delayed when restarting in winter. The high pressure switch requires manual reset.
7.2	The circuit will also include an oil separator to guarantee oil return to the compressorand reduce the risk of shutdown, plus a liquid separator.
8	**Air flow configuration**

8.1	**In** the InRow versions, the air to be cooled is taken in at the rear of the unit, directly from the hot aisle of the data center (35°C), with considerable benefits both in terms of energy efficiency and cooling capacity; it is then cooled and delivered into the coldaisle (18-20°C), that is, the front of the same racks where the air is taken in from.
8.2	The surface of the evaporator coil must be designed to deliver a high level of sensible cooling capacity, i.e. the SHR (Sensible Heat Ratio, ratio between sensible and total heat load) must be > 0.9, measured at an air inlet temperature of 35°C and 30% relative humidity.
9	**Energy Efficiency**
9.1	In order to provide best advantages in terms of energy saving, the CRAC efficiency shall increase when heat load reduces (partial load) or any time the cooling capacity exceeds the required capacity (for instance when outdoor temperature drops).
10	**Control of the condensation stage**
10.1	The condensation stage must be controlled by measuring the compressor dischargepressure i.e. on the condensing unit, so as to be able to manage the effective pressure difference across the compressor and allow simultaneous control of the evaporator-condenser system.
10.2	The condensation stage must be controlled by modulating the power supply voltageto the fans on the outside condenser.
11	**Active redundancy and shared mode**
11.1	The cooling units will be capable of providing active redundancy. To ensure this, all the units installed, including the redundant unit, must be able of operate at the sametime and at part loads.
11.2	This feature must also be able to increase system efficiency by reducing energyconsumption at part loads.
12	**Protection function for long refrigerant lines**
12.1	The unit will have a function that at regular intervals increases gas flow speed, so asto allow better oil return to the compressor even on very long refrigerant lines.
13	**Fans**
13.1	The air-conditioning unit will have EC fans.
13.2	The unit controller will be able to modulate fan speed at part loads, together with the compressor inverter. This further reduces power consumption during part-load operation.
13.3	The fans are designed to allow **"hot replacement"** in the event of faults, i.e. an individual faulty fan can be replaced without having to stop the entire unit, thusreducing system down time.
14	**Power supply**
14.1	The electrical panel should be located such a that it will be easily accessible and away from the air flow. This will be constructed and wired in compliance with standards and will include: contactors and overload protectors for compressors and fans, PCB, and safety devices.
14.2	The unit shall have inbuilt/ external automatic transfer switch with redundant power supply.
15	**Controller with microprocessor**

15.1	The control system will include a microprocessor that will be programmed to manageall the functions of the air-conditioner. The system will include
15.1.1	• An electronic board housing the microprocessor, fitted inside the electrical panel.
15.1.2	• A user terminal as the interface.
15.2	The electronic board complies with EEC directive.
16	**The main functions of the control system are to:**
16.1	• control room temperature
16.2	• manage the compressor;
16.3	• manage fan speed;
16.4	• monitor supply air temperature;
16.5	• manage alarms and warnings for correct maintenance;
16.6	• log up to 100 events;
16.7	• manage the unit in standby;
16.8	• control room humidity
16.9	• allow remote monitoring and control of the unit via LAN, network or BMS (LonWorks, BACnet, Modbus…..).
17	The controller with **password protection** and can manage the following parameters:
17.1	• readings of sensors and probes and corresponding settings;
17.2	• activation of alarms, event log, digital output settings;
17.3	• LAN management;
17.4	• BM communication parameter settings;
17.5	When connected via LAN to other units - up to 10 - the controller can:
17.5.1	• manage, based on set times or events, automatic rotation of the unit/units instandby (1 or 2) ;
17.5.2	• manage the average temperature and humidity between the units;
17.5.3	• access all the control boards from just one remote user terminal,
17.6	In order to protect the software against incorrect settings, some parameters areprotected by **2 password levels**: User lever and Authorised service level.
17	**Filters**
17.1	Regenerable polyester fibre filtering media treated with synthetic resins, supportedby a frame with protective metal mesh.
18	**Noise**
18.1	The units must be designed to reduce noise emissions.
19	**Reheating**
19.1	The unit will be equipped with electric heaters, to allow temperature control during dehumidification cycles.
20	***Humidifier***
20.1	The unit will read the relative humidity (RH) and control the level by activating humidification cycles only when the return air humidity is too low (<40%, settable).

20.2	The humidifier is an immersed electrode model with modulation of steam production. It also features automatic control of dissolved salt concentration so as to allow untreated water to be used
21	***Communication boards***
21.1	The unit will be fitted with RS485 communication board for ModBus protocol.
22	***Alarm sensors :***
22.1	Dirty filter sensor: this sensor is needed to optimise filter operation, so they can bereplaced only when necessary
22.2	Flood sensor: this sensor is needed if there is condensate water spillage outside unit

Modular UPS Requirements & Features

UPS System design concept is based on redundancy and availability, with true double conversion - online system. To support the dual bus system configuration, two units of UPS should be installed. The expansion area should be having two UPS system one on each bus. Dual redundant UPS systems will take care of following needs:

1 Servers/ Network Devices

2 Access Control / Fire Detection, suppression / surveillance system

The solution should be automatic with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source for the Data Centre. Earthing should be provided from the electrical room control panel to the Earthing pits.

The UPS shall have N+1 redundant, scalable architecture. The system power train shall be comprised of hot swappable / user replaceable UPS modules, which shall operate in parallel, and be configured for N+1 redundant operation at rated load. Each UPS module contains a full rated input rectifier / boost converter (hereafter referred to as Input Converter), full rated output inverter, and 10% battery charging circuit. 3 phase power modules with self- testing capability connected to the main power frame.

Technical Specifications of UPS

S. No.	TECHNICAL SPECIFICATIONS
	GENERAL FEATURES:
1	Supply, installation and commissioning of 2 x 180 KVA True On-Line Double Conversion, modular UPS. The 2 x 180 KVA UPS System shall be configured in parallel redundant mode (1+1) configuration without any modification.

2	Each 180 KVA redundant UPS shall be with modular architecture with appropriate nos. of 20, 30 or 50KW Hot Swappable Power Modules of double conversion configuration, i.e. 9 nos modules in case of 20 KW Modules or 6 nos modules in case of 30 KW Modules or 4 nos modules in case of 50 KW Modules. The 180 KW UPS shall be scalable upto 300 KW redundant within the same frame simply by inserting additional hot swappable power modules as and when necessary.
3	The frame for Each 180 KVA UPS shall be in a space saving design, with standard30~42U frame
4	Each hot swappable UPM power module shall include a rectifier, battery converter, inverter and independent logic circuitry. There should be no common controller(either single or redundant) outside the modules.

5	Each UPS shall also have an
	a) STS Module comprising of a fully rated, continuous duty static bypass switchfor high-speed transfers along with RS232 port, USB port, SNMP Slot, Dry contact ports
	b) Switch Unit comprising of Main Breaker, Maintenance Bypass and Output Breaker

6	The control panel comprising of a graphical LCD DISPLAY, touch screen based, with LED status indicators for monitoring of all measured parameters, UPS and battery status and alarms.
7	**BATTERIES: Each 180 KW UPS shall have battery bank comprising of 1,44,000 VAH using 2V, VRLA Sealed Maintenance Free Batteries for 15 minutes backup time. The vendor has to supply the necessary battery rack and interconnecting cables.**
9	**DETAILED SPECIFICATION SHEET**
	MODEL RATING (1.0 p.f.) — 180 KVA/KW Modular On-Line UPS

10	**ELECTRICAL CHARACTERISTICS INPUT**	
	Rated input voltage	380 V; 400 V; 415 V, 3 Phase
	Voltage tolerance	340 ~ 475 VAC @100% load
		240 ~ 475 VAC @50% load
	Rated input frequency	50 or 60 Hz, user configurable
	Frequency tolerance	45 to 55 Hz
	Input power factor, double conversion @100% load	> 0.99
	Input current distortion at rated input current	< 3%, 100% load
11	**ELECTRICAL CHARACTERISTICS**	
	OUTPUT	
	Crest factor	3:01
	Rated output voltage	380 V; 400 V; 415 V, configurable
	Output voltage variation, steady state	± 1% (balanced load); ± 2% (unbalanced load)
12	**Total voltage harmonic distortion**	

	100% linear load	< 2%
	100% non-linear load	< 5%
	Rated output frequency	50 or 60 Hz, configurable
	Output frequency variation	± 0.1 Hz
	Overload capability	10 mins: 110%, 1 min: 125%, 10 seconds:150%
	Efficiency in double-conversion, rated linear load	>95%
13	**BYPASS**	
	Type of bypass	Static
	Bypass voltage range	380 V; 400 V; 415 V
14	**BATTERY CHARACTERISTICS**	
	Battery technology	2V, VRLA SMF Batteries
	Nominal VAH capacity	1,44,000 VAH for 15 minutes Back-up
	Battery start option	Yes
15	**COMMUNICATION CIRCUITS**	
	Standard connectivity ports	USB, RS-232, Web and SNMP card
	System Display	Touch based graphical LCD display
	Centralized UPS Monitoring & Management System	The proposed UPS shall have Centralized UPS Monitoring & Management system comprising of hardware and software, for real-time device monitoring and notification
16	**ENVIRONMENTAL**	
	Acoustic noise at 1 m, in 25 °C ambient temperature	< 75 dBA
	Ambient service temperature range	0°C to + 40°C without output power derating
17	**COMPLIANCE WITH STANDARDS**	
	Quality	ISO 9001, ISO 14001, ISO 45001, ISO 50001
	Safety	IEC 62040-1
	EMC	IEC 62040-2

5 KVA UPS Features

Sl. No	Parameter	Required Specifications
1	**Configuration**	2 x 5 KVA On-Line UPS System in parallel redundant mode with individual battery bank for 30 mins back-up. UPS System should be based on IGBT technology.
2	**Capacity**	**5 KVA** / 5 KW
3	**AC Input Voltage Range**	160-275 V AC, 1 Phase
4	**Input Frequency**	50Hz ± 10% (Suitable for Generators)

5	**AC Output Voltage**	230 V AC, 1-phase ± 1% (Sine Wave Output)
6	**Output Frequency**	50 Hz ± 0.05 Hz
7	**Overload Capacity**	125% for 1 minutes, 150% for 30 seconds
8	**Harmonic Distortion**	<2% for Linear Loads and <5% for non-linearloads
9	**Crest Factor**	3:1 or better
10	**Efficiency**	>90%
11	**Indications & Audible Alarms**	Mains On, Inverter On, Overload, Load OnMains, Load On Battery, Battery Low
12	**Digital Metering**	LCD display for measurement of AC Voltage, Battery voltage, Battery Current, Load Current, Output frequency.
14	**Battery Back-up & Other Details**	The system must be capable of providing requisite battery back-up time of **30 Minutes** using 12V, VRLA Sealed Maintenance Free Batteries with each UPS.
		Required VAH : **4600 VAH for 30 minutes battery backup**
		Individual Battery Capacity must not be lessthan 12V, 26 AH
15	**Certification**	§ **ISO 9001, ISO 14001, ISO 45001** certified.
		§ **CE** (confirming to IEC 62040-1 & IEC62040-2 Standards) & **RoHS Compliance**
		§ **BIS**

Diesel Generator Set

Presently installed DG set which is 200KVA x 3 Nos is to be replaced with 400KVA x 3 Nos(2 running and 1 standby) with required size DG set and sync panel foundation.

DG set sync panel is also to be replaced to cater 400 KVA x 3 Nos of DG set accordingly.

Note: Bidder to arrange for alternate power / Mobile DG Set during replacement / upgradation of exiting DG sets and DG Sync Panel so that there is no downtime to the running of the Data Center. The bidder may visit the site physically and accordingly decide to extend/modify the existing platform for placing the new/upgraded DG sets. It is further clarified that the cost of DG sets offered shall be quoted considering the replacement of existing DG sets.

Sr.	Description
	Diesel Generator Set

1	The total cumulative load of the DG Set after calculating the load of UPS, PAC, and Lighting etc of the existing and new expansion area shall not be less than 800 KVA.The DG Set solution should be in N+1 configuration (where N should be greater thanor equal to 2 Nos with the best rating as per the proposal submitted for redundant purpose. The diesel generator set should be in N+1 redundancy mode. Supply shall be complete with engine, alternator, base frame, acoustic enclosure, fuel tank, residential silencer, exhaust pipe and AMF panel, self starter, battery etc. etc. complete in all respects. All components (excluding AMF panel silencer & exhaust pipe) shall be accommodated in enclosure. Brief specification of various components shall be as under and makes as indicated in the list of acceptable makes.
2	**Diesel Engine:** The Engine shall be water cooled, electric starting, Naturally Aspirated/ turbo charged, 1500 RPM, four stroke multiple cylinder, diesel operated confirming to relevant BS/ IS standards with Dry Type Air Cleaner, Compact Radiator with Recovery Bottle and Pusher type Fan, Engine with Coolant, Engine mounted panel with wiring harness, Holset Coupling and Industrial Silencer, as per engine manufacturers design standards.
3	**ALTERNATOR:** The alternator shall be synchronous, brush less developing required load continuously at 1500 RPM generating 415 volts 0.8 power factor, 3 phase, 50Hz AC supply. The alternator shall be self excited, self regulated and foot mounted directly coupled to the engine with flexible coupling. The alternator shall conform to relevant BS: 5000/ IS: 4722/ IEC 60034-1 standards. The alternator winding shall have class H insulation and bearing shall be ball and roller type permanently lubricated. The alternator excitation system shall be complete with automatic voltage regulator having fast response to load changes.
4	**Base Frame:** Sturdy, fabricated, welded construction, channel iron Base Frame formounting the above Engine and Alternator.
5	**AMF PANEL:** The AMF panel shall be manufactured by firm having CPRI certificate and shall be designed to provide complete protection to engine, alternator and starting and stopping DG set automatically on mains failure/ resumption. The panel shall be accessible through a separate door and shall be suited to min 800 KVA capacity of DG Set. There should be a common AMF Panel for all the numbers of units of DG Set proposed by the bidder.Existing AMF panel which supporting existing 200KVA x 3 Nos of DG sets is to be upgraded or replaced with new AMF panel for newly proposed DG sets.
6	DG Set should be integrated with BMS.
7	**ACCOUSTIC ENCLOSURE:** The enclosure shall be fabricated out of 16 SWG CRCA/M.S. sheet and shall be of bolted construction type. The enclosure shall be powder coated after 7 tank treatment process. The enclosure shall accommodate complete DG set including fuel tank, batteries etc. the insulation inside the enclosure will be provide with fiber glass/ minerals wool and sound level shall be finished with perforated CRCA/M.S. sheet duly powder coated. Adequate number of doors with handed & locking arrangement shall be provided for accesses to various componentsof the DG set. Blower shall be provided for ventilation so that DG set can deliver desired output. The power shall be connected with load side of the AMF Panel and shall continue to operate for 5 Minute after stopping the engine for discharging heat.

8	**FUEL TANK:** Necessary liters capacity inbuilt Fuel Tank with mounting brackets with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return. Also there is a common fuel tank available which need to be integrated with proposed DGsets.
9	**BATTERY:** Dry Maintenance free batteries with leads and terminals.
10	**SILENCER & EXHAUST PIPE:** The silencer shall be residential type and may be installed out side the enclosure. The exhaust pipe shall extended from the DG set to required height above the enclosure Fibre glass insulation 50mm. Thick with aluminum cladding 1 mm. Thick shall be provided on the entire length of exhaust pipe. Metallic bellows shall be provided for vibration isolation. The load of the exhaust pipe & silencer shall not be transferred to the enclosure of D.G. Set. Suitable support from ground level with G.I. pipe/M.S. girder shall be provided.
11	**Space for installation of DG Set:** There are existing 200KVA x 3 Nos of DG set installed at the basement of the SDC building the same needs to be buyed back and new 400KVA x 3 Nos of DG Sets to be installed in this open area near the 1st Floor of the SDC Building.

Server Rack 42U

Sr.	Description
1	19 Inch 42U racks shall be used in the Data Centre. All the racks should be mountedon the floor with castor wheels with brakes.
2	Rack should confirm to DIN 41494 and EIA-310 Standard
3	OEM Should have ISO 9001 certification
4	Front and Back doors should be perforated with at least 63% or higher perforations.
5	All racks should be OEM racks with Adjustable mounting depth, Multi-operatorcomponent compatibility, Numbered U positions, Powder coat paint finish and Protective grounding provisions.
6	All racks should have 2 Nos of Metered PDU's with min 15 Nos of IEC C13 and 4 Nosof IEC C19 sockets with 32A IEC-309 Industrial connector
7	Power Strips in Racks: Two power strips per Racks connected to the separateindustrial socket one from UPS-1 and the other from UPS-2.
8	Each rack should have Temperature & Humidity Sensor integrated with BMS Solution.
9	Mounting hardware 4 Packs
10	All racks must be lockable on all sides with unique key for each rack
11	Racks should be compatible with floor-throw/front throw/top-throw data centre cooling systems.
12	Hot / Cold Containment should be proposed
	Server Rack 42U (600 mm x 1000mm)
	All Server Racks should have the following things in addition to the above mentioned hardware
1	Racks should have Rear Cable Management channels, Roof and base cable access

2	**Wire managers**
2.1	Two vertical and four horizontal
3	**Blanking Panels**
3.1	All 42 U's should be installed with Blanking Panels
9	**Door**
9.1	The racks must have steel (solid / grill / mesh) front / rear doors and side panels.Racks should NOT have glass doors / panels.
9.2	Both the front and rear doors should be designed with quick release hinges allowingfor quick and easy detachment without the use of tools.
10	**Fan trays**
10.1	With 4 fans
11	**Dimensions**
11.1	(Width x Depth) - 600 mm x 1000 mm
12	**Metal**
12.1	Aluminum extruded profile
13	**Side panel**
13.1	Detachable side panels

Network Rack 42U

Sr.	Description
	Network Rack 42U (800 mm x 1000mm)
	Overall specifications:
1	Racks should have Rear Cable Management channels, Roof and base cable access
2	**Wire managers**
2.1	Two Vertical Each at Front & Back and Four horizontal
3	**Blanking Panels**
3.1	All 42 U's should be installed with Blanking Panels
4	**Door**
4.1	The racks must have steel (solid / grill / mesh) front / rear doors and side panels.Racks should NOT have glass doors / panels.
4.2	Both the front and rear doors should be designed with quick release hinges allowingfor quick and easy detachment without the use of tools.
5	**Fan trays**
5.1	With 4 fans
6	**Dimensions**
6.1	(Width x Depth) - 800 mm x 1000 mm
7	**Metal**
7.1	Aluminum extruded profile
8	**Side panel**
8.1	Detachable side panels

IP KVM Switch

Sl.No.	Specifications
	IP based Keyboard, Video Display Unit and Mouse Unit (KVM) and/or otherControl Devices/PCs may be used for the IT Infrastructure Management forwhich the necessary consoles/devices shall be placed in the location earmarked as Administration Area where the Admin staff will be seated. The KVM unit should provide the following functionalities:
1	It should be rack-mountable
2	It should have 24 ports
3	It should support local user port for rack access.
4	The KVM switch should be SNMP enabled. It should be operable fromremote locations.
5	Should have a min 15 inch LCD monitor
6	It should support multiple operating system
7	It should have serial device switching capabilities
8	It should have dual power with failover
9	It should support multi-user access and collaboration

LED Display

Sr No.	Specification	Detail
1.	Display Resolution	Ultra HD (3840 x 2160)
2.	HD format	4K UHD
3.	Screen Size	53 inch or higher
4.	Backlight	LED/OLED
5.	Display Colour	>1 billion colours
6.	External Connections	Display Port - 1, HDMI - 2, USB - 2, RJ45, WiFi
7.	Display Control	IR, LAN, Keypad
8.	Orientation	Portrait & Landscape
9.	Speakers	Built-in or external

10.	Operating Temperature	0° to +40°C
11.	Options / Features	On/Off scheduling, Pre-sets
12.	Accessories	Power cord, HDMI 10 mtrs cable, remote control, floor mount stand / wall mount kit / pedestal (as persite requirement)

Desktops

Sr. No.	Item Description	
	Models:	
1.	Processor	Intel Core i5, @2.9Ghz or higher, 12MB cache, 10th GenerationProcessor or higher or equivalent
2.	Operating System	Windows 10 Pro 64 bit or higher.
3.	Memory	16 GB DDR4-2666 MHz or higher, having 2 DIMM Slots
4.	Storage	1TB HDD (7200 RPM or above)
5.	Optical Device	DVD R/W drive
6.	Graphics	Intel Integrated HD
7.	Security	TPM 2.0 or higher
8.	I/O Ports	2 x USB 3.0, 2 x USB 2.0, 2 x audio/ universal port, VGA, HDMI x 2, 10/100/1000M Gb IPV6 Compliant LAN
9.	Certifications	Energy Star 6.0 or better, EPEAT Gold/ EPEAT Registered
10.	Keyboard	104 Keys OEM English Wireless Keyboard same brand as that of PC
11.	Mouse	Plug-and-play Wireless mouse same brand as that of PC
12.	Speaker	Internal/external speaker 2 X 2 Watts. Or higher
13.	Monitor	21.5" or higher antiglare LED display color monitor, FHD (1920 x 1080), EMI/FCC (or ETDC Report for meeting FCC norms) compliance, Energy Star 6.0 or higher compliance, monitor of same brand as that of PC
14.	Connectivity support	802.1 1b/g/n/ac / 802.11bgn, Bluetooth 4.0
15.	Warranty	Five years comprehensive onsite warranty.

ELECTRICAL :

Existing transformer Output Panel is located approx. 60 meters away from DC building. which is feeding Phase-1 Data Center setup has 400 Amp MCCB. This MCCB is to be replaced and upgraded

with 1000 Amp MCCB. And also accordingly, bus bar inside the transformer Output panel is to be upgraded with 1000 Amp current carrying capacity. This panel will also provide power supply to new proposed Phase-2 DC setup.

New MCCB of 1000 Amp is to be provided along with busbar extension and panel for proposed Phase-2 DC setup.

Bidder has to check the Panel and propose if the Transformer Output Panel can be upgraded or is to be replaced with the New Panel. The cable from Transformer output panel is to be layed till ground floor electrical room of SDC building (which is approx. 60 meters away).

The electrical cabling Work shall include the following:

- Electrical panel in Data Center for UPS's, InRow Cooling Units and Comfort AC distribution
- Power cabling
- Dual distribution path for DG, UPS etc.
- UPS Distribution Board
- UPS point wiring
- Power Cabling for Utility component and Utility Points etc
- Online UPS
- Separate Earth Pits for the component

The distribution of power from the UPS room to the following shall be considered:

- All proposed component for the production environment
- UPS of minimum 180KVA = 180KW in N+1 redundancy with static bypass arrangement
- Sub distribution panels for UPS
- Final Distribution shall be through Floor Mounted Power Distributions Units with suitable sized K-13 Isolation Transformer (PDU). Power in the racks and other component's shall be provided with two sockets with power coming from separate UPS in each of these sockets.
- The PDU should be designed for distribution of power up till rack level keepingin mind the number of termination required for the entire server farm area. It is mandatory that at least 10 percent of free MCB in each PDU may be availablein case of failure of any connection. Two separate connections to the rack should be provisioned for the Rack power distribution, one from PDU-1 (Source UPS 1) and the other in PDU-2 (Source UPS-2).
- Static Switch (STS) should be planned for the IT equipment's where there is no provision

of redundant RPS, the equipment's like L2 switches, Firewall, IPS etc may be considered. (The basic purpose of a static switch is that is takes the power from 2 sources and output it as one, it has an inbuilt automatic bypass switch which will enable any one source to be enabled and if one goes downthe other input starts working which will give a uninterrupted power at the output

LT Electric Panel Boards

I. The main LT Panel board shall be extendible type on both sides, having in it all switches, starters & accessories and shall be completely factory prewired. It

shall be suitable for voltage systems up to 500 volts, 3 phase, 50 Hz, 4 wire supply capable of functioning satisfactorily in temperatures of 45 degree Celcius and suitable capacity at 415 Volts.

II. The switch board shall be dust proof and vermin proof. The panel shall generally conform to IS 8623. The panel shall have front/rear access.

III. Cable compartment of adequate size shall be provided in the main distribution board for easy termination of all incoming and outgoing cables entering from bottom or top. Adequate support shall be provided in cable compartment to support cables. All incoming and outgoing switch terminals shall be brought out to terminal blocks in cable compartments.

IV. The doors of the switch compartments and cable access shall be hinged type and that of busbars shall be fixed type.

V. The panel mounted lock shall be provided with a locking arrangement.

VI. All panel doors shall have synthetic rubber gaskets with good ageing, compression and resistance characteristics.

VII. All the breakers shall be interlocked with door so that the unit cannot be closed unless the unit door is closed. The interlock shall also prevent opening the unit door unless the switch/breaker is in OFF position.

VIII. Defeat arrangement shall be provided for deliberate inspection of switch/ breaker without having to switch OFF the unit.

IX. A danger notice plate of 200 mm x 150 mm of mild steel at least 2 mm thick vitreous enameled white on both sides and with inscriptions in signal red colour on front side shall be provided on the panel board.

X. Every starter/contactor etc. shall be controlled by an isolating device of adequate rating.

XI. A voltmeter and ammeter shall be provided to indicate incoming voltage and along with rotary phase selection switches.

XII. LED type indicating lamps in approved colours shall be provided for the 3phases and for status of all controlled devices.

XIII. All the switchgear shall be earthed to the earth bus.

XIV. Earth shall be extended for each compartment to the door by means of aflexible, insulated copper conductor with crimped legs on either side.

XV. Each panel shall be provided with suitable size of earth bus at the rear of thepanel

and two earth terminals on either side.

XVI.   Suitable printed PVC ferrules shall be provided for all the conductors for easy identification.

XVII.   Etched plastic name plates shall be provided for all the incoming, outgoing switchgears, ammeter, voltmeter etc.

XVIII.   All the control and auxiliary wiring shall be carried out with PVC insulatedcopper conductor of proper colour code.

XIX.   The power wiring from the circuit/air breakers to the starters shall be carriedout using colour coded, PVC insulated copper conductors crimped with lugs.

XX.   The outgoing wires of starters shall also be PVC insulated colour coded copper conductor crimped with lugs and terminated on a terminal block of proper rating.

Bus Bars

I.   The Bus Bar shall be mounted in a separate compartment in the Panel Board.

II.   The Bus Bars and interconnections shall be of aluminum strips unless otherwise specified.

III.   The Bus Bar shall have rectangular cross - section of 1 sq.mm per Amp rating for full load current in the 3 phases as well as for neutral and should be extendable.

IV.   The Bus Bars shall be insulated with heat shrink sleeves and colour coated. They should be supported on supports made of glass fibre reinforced thermosetting compound at regular intervals sufficient to withstand the force of any short circuit.

Circuit Breakers

The panel and the bus bars plus outgoing of all devices shall be protected by differenttypes of circuit breakers.

Air Circuit Breaker (ACB)

I.   The air Circuit Breakers shall be Draw out type conforming to I.S: 13947 (Part2) 1993.

II.   The ACB shall be complete with solid state overload, short circuit and earthfault protection with adjustable settings.

III.   Each ACB shall have 4 "NO" and 4 "NC" potential free auxiliary contacts, in addition to those required for its internal operating mechanisms.

IV.   There shall be suitable indicators for OPEN/CLOSE/SERVICE/TEST andspring charged positions.

V.   It shall be possible to close the door in Test position.

VI.   Castle Key and/or other interlocking devices shall be provided as required

Moulded Case Circuit Breakers (MCCB)

I. The MCCB shall have TP + NL and be suitable for simultaneous manualopening and closing with rotary operating handle.

II. The ON/OFF/TRIP positions shall be clearly marked and easily visible to an operator and confirm to latest IS: 13947-1993.

III. There shall be fixed/adjustable tripping devices with inverse time characteristics for overload and short circuit protection.

IV. Suitable Interlocking mechanism shall be provided, where required.

2.2.5.1 Miniature Circuit Breakers (MCB)

I. The MCB shall have quick make/break contacts with a heat resistant housing,having high Impact strength and confirm to IS 8828-1996.

II. The contacts shall be of silver nickel alloy.

III. The MCB shall permit over load for short duration, as required for Inductiveloads and the breaking capacity shall not be less than 10 KA at 415 Volt A.C.

IV. It shall be equipped with overload and short circuit protection devices and shallbe suitable for DIN mounting.

2.2.6 Painting

All sheet steel work shall undergo a multi tank process of degreasing, pickling in acid, cold rinsing, phosphating, passivating and then sprayed with a high corrosion resistant primer. The primer shall be baked in oven. The finishing treatment shall be by application of powder coated paint of approved shade and stoved.

2.2.7 Specifications for Electrical Cabling

FRLS cables of rated capacity exceeding the power requirement of fully blown configuration of the existing and proposed component to be used. For expansion needs suitable redundant power points to be provided at suitable locations. All materials used shall conform to IS standards as per industry practice.

*   Bunching of Wires — Wires carrying current shall be so bunched in the conduit that the outgoing and return wires are drawn into the same conduit. Wires originating from two different phases shall not be run in the same conduit.
*   Drawing of Conductors — The drawing Aluminum / Copper conductor wires shall be executed with due regards to the following precautions while drawing insulated wires in to conduits. Care shall be taken to avoid scratches and kinks, which cause breakages.
*   Joints — All joints shall be made at main switches, distribution boards, socket outlets,

lighting outlets and switch boxes only. No joints shall be made inside

conduits and junctions boxes. Conductors shall be continuous from outlet to outlet.

- Mains & Sub-Mains — Mains & sub-mains wires where called for shall be of the rated capacity and approved make. Every main and sub-main shall be drawn into an independent adequate size conduit. Adequate size draw boxes shall be provided at convenient locations to facilitate easy drawing of the mains and sub-mains. An independent earth wire of proper rating shall be provided. The earth wires shall run along the entire length of the mains and sub-mains.
- Load Balancing — Balancing of circuits in three-phase installation shall be planned before the commencement of wiring.
- Color Code of the Conductors — Color code shall be maintained for the entire wiring installation, Red, Yellow, Blue for three phases and —OFF‖ circuit blackfor neutral and green for earth (or bare earth).
- Fixing of the Conduits — Conduits junction boxes shall be kept in position and proper holdfasts shall be provided. Conduits shall be so arranged as to facilitate easy drawing of the wires through them. Adequate junction boxes of approved shape & size shall be provided. All conduits shall be installed so asto avoid stream and hot water pipes. After conduits, junction boxes, outlet boxes & switch boxes are installed in position their outlets shall be properly plugged so that water, mortar, insects or any other foreign matter does not enter into conduit system. Conduits shall be laid in a neat and organize manner as directed and approved by the Information Technology Department Personnel or person on their behalf. Conductors shall be planned so as not to conflict with any other service pipe lines / ducts.
- Protection — To minimize condensation or sweating inside the conductors all outlets of conduit system shall be adequately ventilated and approved by the proper competent authority. All screwed and socket connections shall be adequately made fully water tight by use of proper jointing materials.
- Switch-Outlet Boxes and Junction Boxes — All boxes shall conform to all prevailing Indian Standards. The cover plates shall be of best quality Hylam sheets or ISI grade Urea Formaldehyde Thermosetting insulating material, which should be mechanically strong and fire retardant. Proper support shall be provided to the outer boxes to fix the cover plates of switches as required. Separate screwed earth terminals shall be provided inside the box for earthing purpose.
- Inspection Boxes – Rust proof inspection boxes of required size having smooth external and internal Finish shall be provided to permit periodical inspection and to facilitate removal and replacement of wires when required.
- Lightning protection to Data Centre
- Surge protection

PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for nonmetallic conduit 1.6 mm thick as per IS 9537/1983.

- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they canremain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E, regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system, shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

Wiring

- PVC insulated copper conductor (FRLS) cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Colour code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reductionof strands is permitted at terminations. No wire smaller than 3.029 sq.mm shall be used.

- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D. B number shall be used for sub main, sub circuit wiring .the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.

- Circuits fed from distinct sources of supply or from different distribution boardsor M.C.Bs shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of dia cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associates switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line exceptingat the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts The earth continuity insulated copper wire in Green colour shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs andswitch boxes with proper lugs as required maximum number of PVC insulated 650 / 1100 grade copper conductors cable which can be drawn in a conduit.

Earthing

- All electrical components are to be earthen is to by connecting two earth tapes from the frame of the component ring will be connected via several earth electrodes. The cable armour will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS- 3843-1986. All the applicable IT infrastructure in the Data Center shall be earthed.
- Earthing should be done inside the Data Centre for the entire power system and provisioning should be there to earth UPS systems, Power distributionunits, AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel

& protect the equipment from voltage gradients which are likely to damage the equipment.

- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- All proposed new earthing shall be Copper / GI maintenance free chemical earthing.
- Provision of earthing for existing as well as new equipment supplied shall be in the scope of SI.

Electric cabling

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct .Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a crisis crossing is avoided and final take off to switch gear is easily facilitated.
- All the Cables shall be FRLS type.

- All cables will be identified close to their termination point by cable number asper circuit schedule. Cable numbers will be punched on 2mm thick aluminium strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthing arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.

Electrical Lights

The electrical lights proposed in the Server Room and UPS & Electrical Room shouldbe equipped with occupancy sensors to conserve electricity. Additionally, it is also proposed to have LED Lights in State Date Centre to enable low power consumption and reduce cooling loads in the critical areas of Server Room. The LED light fixtures should come with following features:

1. Easily dimmable, Instant-On, no flicker or noise
2. Lifetime of at least 50,000 hrs
3. Easy integrate feature in false ceiling or wall surface
4. Products should be backed with 5 year product warranty

Structured cabling:

- All required cables should be laid up to the rack level in the Data Centre.
- Dedicated raceways / cable-trays should be used for laying LAN.
- Doing cabling as required in project duration is responsibility of DCO
- All the cable raceways shall be adequately grounded and fully concealed withcovers.
- The cables should be appropriately marked and labeled.

- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data
- Cabling between the racks should be done using OFC and cabling in the racks should be done using CAT 6A/7 cables.
- All cabling must be done as per the EIA/TIA 942 Data Centre Cabling Standards
- Cabling for minimum 24 ports per Rack for both Copper and Fiber.

Data Cabling

Specification for CAT 6A Cabling System

Sr.	Standard Compliance
	Channel Performance
1.1	The Category 6A/ Class EA UTP SCS shall comply with the following standardsISO/IEC 11801:2010, ANSI/TIA-568-C and IEEE 802.3 applications.
1.2	The Category 6A/ Class EA UTP system should support the following IEEEthernet applications 802.af and 802.3at.
1.3	Should support a minimum of 4 connector Channel with a minimum 3 dbguaranteed NEXT margin.
1.4	The Category 6A cable and Category 6A channel components shall be manufactured by a single manufacturer. The manufacturer shall warrant the Category 6A channel cable, components, and applications for a period of 25 years.
1.5	The Category 6A system should support channels that are shorter than 15 metersfor 4 connector channels without any minimum length requirements. ETL 4 connector report shall be submitted.

Specification for CAT 6A LSZH U/UTP Cable

2.1	The Cable should meet ANSI/TIA 568C.2 Category 6A Specifications
2.2	Cables should have a unique Serial Number printed on the jacket to check the Genuity / details of the test reports. The customer should be able to download the factory test reports of the cable through an online system that can be accessed at any time publicly.
2.3	The cable should consist of Eight 23 AWG solid copper conductors.
2.4	It should support Operating temperature of -20 to 60 ^{0}C
2.5	Should have ETL verified Certificate
2.6	The LSZH Cable should support the following standard to qualify ISO/IEC 60332- 3-22 Flame spread test (Test for a bunch of cables), ISO/IEC 60754-2 Acidity and ISO/IEC 61034-2 Smoke Density.
2.7	The cable and cordage shall be UTP components that do not include internal orexternal shields, screened components or drain wires.

Specification for Category 6A U/UTP Information Outlets

	Standard Compliance
	Category 6A - 10Gigabit outlets
3.1	The 8-pin modular (RJ-45) jacks shall comply with IEC 60603-7-4
3.2	The Category 6A outlets shall be backward compatible with Category 6 and 5Ecords and cables.
3.3	The Category 6A outlets shall support T568 A & B wiring.
3.4	The information outlet must support 90 degree cable termination. For terminatingin areas where the space is a constraint.
3.5	The information outlet will have insertion life of 750 cycles minimum.

Specification for CAT 6A LSZH U/UTP RJ45 Patch Cords

	Standard Compliance
	Modular RJ45 Patch Cords
4.1	The Patch cords shall be solid core construction to provide superior performance.
4.2	Cords shall be equipped with 8-pin modular plugs on each end.
4.3	The cord shall be LSZH and must comply with the following Fire Safety standardsISO/IEC 60332-3-22: Flame Spread (for a bunch of cables), ISO/IEC 60754-2: Acidity and ISO/IEC 61034-2: Smoke Density
4.4	The cordage shall be UTP components that do not include internal or externalshields, screened components or drain wires.
4.5	The patch cords will have insertion life of 750 cycles minimum.

Specification for CAT 6A Jack Panel

	Standard Compliance
	24 Port Patch Panel
5.1	The ganged adapter style patch panel will utilize increments of six RJ-45 stylejacks in a common molded component.
5.2	The panel must be capable of supporting an upgrade to an intelligent system without any interruption to service due to patch cord removal or terminal block re-termination.
5.3	The panel should have an integrated rear cable management bar that allowsbunching of 6 cables and properly dressing the cables.
5.4	The panel shall come with Velcro Tape for dressing the cables.
5.5	The panel shall be UL and cUL Listed

CORES - INDOOR OM4 FIBER CABLE

S. No.	PARAMETER	SPECIFICATIONS
1	**Type of Cable**	12F Indoor, OM4, Gel Free, Tight Buffered Cablewith Rip Cord
2	**MINIMUM SPECIFICATIONS**	ANSI/ICEA S-83-596, Telcordia GR-409
3	**FIBER TYPE SOLUTION**	OM4, BEND INSENSITIVE MULTIMODE FIBER
a)	Fiber Size	50/125/250 microns
b)	Jacket Material	Low Smoke Zero Halogen & Riser rated
c)	Total Fiber Count	12 Core
d)	Jacket Color	Aqua
4	**DIMENSIONS**	
a)	Diameter Over Jacket	6.07 mm
5	**PHYSICAL SPECIFCATIONS**	
a)	Cladding Diameter	125.0 μm
b)	Minimum Bend Radius, Loaded	91 mm
c)	Minimum Bend Radius, Unloaded	61 mm
d)	Tensile Load, Long term, maximum	200 N
e)	Tensile Load, Short term, maximum	667 N
6	**ENVIRONMENTAL SPECIFICATIONS**	

a)	Environmental Space	Low Smoke Zero Halogen (LSZH) and Riser
b)	Installation Temperature	-10 deg. C to +60 deg. C
c)	Operating Temperature	-20 deg. C to +70 deg. C
d)	Storage Temperature	-40 deg. C to +70 deg. C
7	**MECHANICAL TEST SPECIFCATIONS**	
a)	Compression	10 N/mm
b)	Compression Test Method	IEC 60794-1 E3
8	**OPTICAL SPECIFICATIONS, WAVELENGTH SPECIFIC**	
a)	Standards Compliance	IEC 60793-2-10, type A1a.3a	IEC 60793-2-10,type A1a.3b	TIA492AAAD (OM4)
b)	Attenuation, maximum	1.00 dB/km @ 1300 nm 3.00 dB/km @ 850 nm
c)	1 Gbps Ethernet Distance	600 m @ 1300 nm 1110 m @ 850 nm
d)	10 Gbps Ethernet Distance	550 m @ 850 nm
e)	Bandwidth, Laser, Minimum	500 MHz-km @ 1300 nm 4700 MHz-km @ 850 nm
9	**REGULATORY COMPLIANCE**	RoHS

U Rack Mounted High Density Fiber Optic Patch Panel

Sr. No.	Specifications
7.1	1 U, high density fiber optic shelf shall be proposed that can be used for acombination of splicing and termination of fiber optic building cable or outside plant (OSP) cables.
7.2	The 1 U height fully enclosed shelves shall include integrated front cablemanagement trough and shall be slide-out type for easy access.
7.3	The Panel shall accommodate 6, 12, 24 or 48 fibers

24 Fiber LC Adapter Plate

Sr. No.	Specifications
8.1	Each module shall accommodate 6 LC Duplex ports.
8.2	Shall be compliant to RoHS
8.3	Shall be UL listed

LC – LC OM4 Multimode Fiber Patch Cord

Sr. No.	Specifications
10.1	The patch cord shall be OM4 multimode fiber compliant to ANSI/ICEA S-83-596 or Telcordia GR-409.
10.2	The fiber cable jacket shall be LSZH complying to IEC 60332-3
10.3	The connector material shall be pre-radiused Zirconia.
10.4	The insertion loss shall not exceed a maximum of 0.24 dB and a minimum returnloss of 27 dB
10.5	The fiber patch cord shall comply to ANSI/TIA 568 C.3 standards.
10.6	The patch cord shall be RoHS 2011/65/EU compliant
10.7	Both connectors of the patch cord shall be LC type

CIVIL AND ARCHITECTURAL WORK

The civil work includes furnishing the data center area in all aspects. The furnishingincludes but not limited to the following:
- Cement Concrete Work
- Cutting and chipping of existing floors
- Trench works
- Masonry works
- Hardware and Metals
- Glazing
- Paint work
- False Flooring
- False Ceiling
- Storage
- Furniture & fixture
- Partitioning
- Doors and Locking
- Painting
- Fire proofing all surfaces
- Insulating

The selected bidder should adhere to the following civil and interior specifications:

Flooring

- Providing & fixing steel cementations raised access floor of FFH up to 450mm finished with antistatic high pressure laminate in size 600 x 600 mm x 35 mmwith point load 450 kg and uniform distribution load (UDL) 1350 kg per sq. meter as per following specifications: Panel Type - M 1000, Understructure- Edge Support Rigid Grid, Wear resistance (g / cm2) - < 0.08, Bottom profile — Hemispherical shape, Pedestal -all steel construction & silver zinc plated, Exposed surface- Special weather coating on entire surface of the tiles. The same should also be provided with wire manager and tile lifter etc.
- At least 1' 6‖ High from existing floor level using antistatic laminated tiles.
- Supply & Fixing of 1.5 mm Antistatic Laminate skirting matching with floor tiles with 8mm thick MDF Board / Bison Board up to a height of 4"
- Providing and fixing 9 mm thick floor insulation below the false flooring andjoints should be finished properly as per manufacturer's specification.

False Ceiling

- Providing and fixing in position gypsum board false ceiling / metal false ceiling with approved G.I / Al / Steel Framework and hangers including openings for lights etc. to be framed with teak wood members at no extra cost etc. as per specification and description complete.
- Providing and fixing 9 mm thick insulation above the false ceiling and joints should be finished properly as per manufacturer's specification. The rate shall be inclusive of cleaning the surface to make it free from dust.

Partitions (wherever applicable)

- Providing and fixing in position 132mm full height with 2 layers of 15mm thick Fireline gypsum board on both side with GI steel metal vertical stud frame of size 70 mm fixed in the floor channels to provide a strong partition. Glass wool Insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The rate shall include making cutouts for switch board, sockets, grill etc. for which no extra will be paid separately The rate shall Include for preparing the surface smoothly and all as per manufacture's specification etc.
- Providing and fixing in position full height partition wall of 75 mm thick plain gyp-board partition using 12.5 mm thick gyp-board on both sides with GI steel metal vertical stud frame of size 48 mm fixed in the floor and ceiling channels of 50mm wide to provide a strong partition. Glass wool Insulation inside shallbe provided as required. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The rate shall include making cutouts for switch board, sockets, grill etc. for which no extra will be paid separately The rateshall Include for preparing the surface smoothly and all as per manufacture's specification etc. Finally finishing with One coat of approved brand of fire resistant coating.

- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- Providing and fixing in position of 75 mm thick plain gyp-board partition using 12.5 mm thick gyp-board on both sides with GI steel metal vertical stud frameof size 48 mm fixed in the floor and ceiling channels of 50mm wide to provide a strong partition. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The joints shall be finished with joint paper tape by using jointing compound of India gypboard Ltd., and applying over it 3 layers of the filler compound to provide a smooth surface. Finally finishing with one coat of approved brand of fire resistant coating. The partition will be mainly to clad the shaft walls.
- All doors should be minimum 4 ft wide.

Painting

- Providing and applying fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendationfor coverage of paint.
- Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.

Civil Work (wherever applicable)

- Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement: 4 sand) with bricks of approved quality chamber bricks of class designation 50
- Providing & making SS signage with text in etched & black painted of Dline make or equivalent to be located as directed (wall mounted) for space nomenclature/ directions.
- Plastering with cement mortar 1:5 (1 cement : 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification.
- Anti-termite treatment of the entire critical area.

Doors

- Emergency exit of Phase-2 Data Center is to be replaced with new fire rateddoor.
- Entry to Phase-2 Data Center from Phase-1 Data Centre door has Panic barthis is to be shifted to Phase-2 emergency exit door.
- New proposed UPS room on ground floor has to be fire rated door.

BMS, FAS, WLD, VESDA, PA etc Technical Compliance

Sr.	Description
	Building Management System (BMS)
	Bidder to visit the SDC Site, check and study the existing installed BMS for Phase1 SDC. If existing system or any of its components are not sufficient to cater to the future load, then only required components / equipment's to be proposed for the proposed new Server Room expansion area in compliance to below mentioned technical/functional requirements.
	The building management system shall be implemented for effective management, monitoring and Integration of various components like HVAC systems, Access Control systems, fire detection system etc. The BMS shall perform the following general functions including but not limited to:
1	Building Management & Control
2	Data Collection & archival
3	Alarm Event & Management
4	Trending
5	Reports & MIS Generation
6	Maintenance & Complaint Management appliances necessary to install the said system, complete with Sensors, Direct Digital Controllers, Communication Controllers and Supervisory Software complete with necessary software/hardware support for interfacing with other systems. It shall include laying of cabling duct, conduits and power supply etc., necessary for installation of the system with supplyof appropriate type products as indicated in the specification and Bill of Quantities. The controller shall be 32 bit based Microprocessor Controller and shall sit directly on the TCP / IP network. The Controller shall be Web Based, Web Enabled, Real Time Clock, and Web Browser with Communication speed min of 10 Mbps. Agencyshall design & provide a full Building automation system on the basis of truly distributed intelligence and shall comprise of the following general functional sub systems.

7	Air Conditioning Management & Control
o	Precision AC Units.
o	Temperature monitoring and controls at all specified positions/locations
·	Energy Management
o	LT Panel Energy Monitoring
o	UPS Monitoring
·	Safety & Security Systems Integration.
o	Fire Alarm System Integration.
o	HSSD (High Sensitivity Smoke Detection System) System Integration.
o	Access Control System.
o	Gas System Integration.
o	CCTV
o	Water leakage Detection System
·	Diesel Generator Integration
o	Fuel consumption
o	Load current
·	43" LED display panel with minimum 1,00,000 contrast ratio for monitoring purposes
	The necessary server, operating system, database etc required for the implementation of BMS in SDC would be provisioned by DCO on its own and costof the same would be built-in the solution proposed by the DCO. No separate line items would be mentioned for these items in the BOM. However, the DCO has to provide necessary licenses to cover all the IT infrastructure installed in the HP SDC during the operation period five years.

Sr.	Description
	Water Leak Detection System
	The water leak detector shall be installed to detect any seepage of water into the critical area (Server Room). It shall consist of water leak detection cable/ tape sensor, detection module and control panel. The cable/ tape shall be installed in the ceiling & floor areas around the periphery.
1	**Water Leak Detection Panel**
	The panel shall be microprocessor based one, and should be modular in design. Thesystem shall have different zones and detectors shall be connected to the panel through the zone module. Each area of the premise shall be divided into specific zones such that the user if required shall isolate any zoneThe Panel shall provide volt free contacts to connect to BMS System.
2	**Water leak detection Module:**

Sr.	Description
	Zone Sensor module is surface mounted below the false floor/ above false ceiling where localized detection is required. The zone Module shall provide monitored circuitry for connection to WLD panel. The Zone Modules shall be housed in suitable housings.
3	**Sensing Cable :**
	Tapes are covered with plastic netting to prevent short circuits when used in metal trays or conduits and shall enable the tape to be folded at right angles to allow easyrouting. Water leak detection tape shall provide for the earliest detection of water accumulation in the false ceiling/ False floor

Sr.	Description
	Public Address System
	Bidder to visit the SDC Site, check and study the existing installed PA System for Phase 1 SDC. If existing system or any of its components are sufficient to cater tothe future load, then only required components / equipment's to be proposed for the proposed new Server Room expansion area in compliance to below mentioned technical/functional requirements.
	The PA system is required for:
§	Making public announcement from the Security Control Room and Facility Manager'sroom. Clear and crisp announcement should reach to the entire Facility area.
§	Microphones should be provided to make announcements / respond toannouncement from the designated location within the Facility.
§	To play light music if required.
1	**Speakers**
§	Input Power required is 6W / 24W Max.
§	Rated voltage should be 70-100V
§	Rated Impedance should be 1667 ohms
§	Effective frequency range (-10dB) - 150 Hz - 15 KHz

Sr.	Description
	Fire Detection and Control Mechanism
	Bidder to visit the SDC Site, check and study the existing installed Fire Panel for Phase 1 SDC. If existing system or any of its components are sufficient to cater to thefuture load, then only required components / equipment's to be proposed for the proposed new Server Room expansion area in compliance to below mentioned technical/functional requirements.
1	**System Description**
.	The Fire alarm system shall be an automatic single loop addressable fire detection andalarm system, utilizing addressable detection and alarm sounders.

·	Detection shall be by means of automatic heat or smoke detectors located throughout the Data Center (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.
2	Control and indicating component
·	The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2/ UL standard for the control and indicating component and EN54 Part 4/ UL standard for the internal power supply.
·	All controls of the system shall be via the control panel only.
·	All site-specific data shall be field programmable and stored in an integral stroage device.
·	All internal components of the control panel shall be fully monitored.
·	The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.
·	The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
·	All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2/ UL standard. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.
·	Cancel fault and display test functions shall be configurable to be accessed from level 1 or level 2.
·	All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
·	The control panel shall log a minimum of 500 events comprising of 100 event fire log and 200 event fault, disablement and historic logs, giving time, date, device reference and status of indication.
·	Fire, fault and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display and the internal supervisory buzzer.
·	The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.
·	All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.
·	The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance

	reminder facility.
·	The system will include a detection verification feature. The user shall have the option toaction a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.
3	Manual Controls
·	Start sounders
·	Silence sounders
·	Reset system
·	Cancel fault buzzer
·	Display test
·	Delay sounder operation
·	Verify fire condition
·	Enter or modify device text label
·	Setup maintenance reminder
·	Assign or modify zones
·	Disable zones, device, sounders, FRE contact, auxiliary contacts
·	Enable zones, device, sounders, FRE contact, auxiliary contacts
·	Action weekly test
·	Disable loop
4	Manual call points (MCP)
·	MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS standard. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS standard, without the need for special tools or the need to unfasten the cover plate.
·	The MCP shall be suitable for surface or flush mounting. When flush mounted thedevice shall be capable of fixing to an industry standard single gang box.
5	Smoke detectors
	Smoke detectors shall be of the optical or ionization or photoelectric type. UL Listed products can also be used.. The detectors shall have twin LEDs to indicate the devicehas operated and shall fit a common addressable base.
6	Heat detectors
·	Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise typewith a fixed temperature operating point.
·	Devices shall be compatible with the CIE conforming to the requirements of EN54 Part5/ UL Standard and be LPCB approved.
·	The detectors shall have a single LED to indicate the device has operated and shall fit acommon addressable base.
7	Addressable detector bases

·	All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including ashort circuit isolator.
·	The device shall be automatically addressed by the CIE on power up of the loop withoutthe need of the insertion of a pre-programmed EPROM or setting of DIL switches.
·	Detector bases shall fit onto an industry standard conduit box.
8	Audible Alarms
	Electronic sounders shall be colored red with adjustable sound outputs and at least 3sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min.

Sr.	Description
	Fire Suppression Systems
	The Clean Agent Fire Suppression system cylinder, CCOE, Nagpur approved seamless cylinders, discharge hose, fire detectors and panels and all other accessories required to provide a complete operational system meeting applicablerequirements of NFPA 2001 Clean Agent Fire Extinguishing Systems, NFPA 70 National Electric Code, NFPA 72 National Fire Alarm Code or ISO standards mustbe considered to ensure proper performance as a system with UL/FM/LPCB approvals and installed in compliance with all applicable requirements of the local codes and standards.
·	The Clean Agent system considered for Total flooding application shall be incompliance with the provisions of Kyoto Protocol.
·	Care should be taken that none of the Greenhouse Gases identified in the KyotoProtocol is used for fire suppression application.
·	The minimum criterion for the selection of the Clean Agent will be on the following parameters:
·	Zero Ozone Depleting Potential.
·	Global Warming Potential not exceeding one.
·	Atmospheric Lifetime not exceeding one week.
·	Fire Suppression Gas must be NOVEC 1230, having no environmental impact
·	The minimum design standards shall be as per NFPA 2001, 2004 edition or latestrevisions.
·	All system components furnished and installed shall be warranted against defects in design, materials and workmanship for the full warranty period which is standard withthe manufacturer, but in no case less than five (5) years from the date of system acceptance
·	Additionally, Portable Extinguishers (CO2 or Halon based Extinguishers are notacceptable) shall be placed at strategic stations throughout the Data Centre.

Sr.	Description
	High Sensitivity Smoke Detection System
	The HSSD system shall provide a early warning of fire in it's incipient stage, analyzethe risk, and provide alarm and actions appropriate to the risk The system shall include, but not be limited to, a Display Control Panel, Detector Assembly, and the properly designed sampling pipe network. The system equipment shall be supplied by the manufacturer or by its authorized distributor.
1	**Regulatory Requirements**
·	National Electrical Code (NEC)
·	Factory Mutual
·	Local Authority having Jurisdiction
2	**System Description**
·	The HSSD system should provide an early warning of a fire in its incipient stage. HSSD Detector shall be installed to sample the air from a protected area. In operation the air from the protected area should be drawn through a piping network in the detector unit by an aspirating fan unit to the detector assembly. The air shouldbe illuminated by a laser light source. Smoke particles should scatter this light to a sensitive solid-state photo sensor. An Analogue signal to be transmitted to the display control panel which displays the smoke obscuration levels in a bar graph display. Each increment in the bar graph should represent 120% of the full-scale sensitivity of the detector.
·	Three independently programmable alarm points should provide additional visual indications on the display control cards and activate associated relays for additional annunciation and alarm. Similar systems, which incorporate a nepholometric type detector and require periodic replacement of the light source unless all the conditions are met, shall not be considered in any manner.
3	**Engineering Sampling Pipe Network**
·	Piping networks shall be laid out to provide detection points with spacing. Pipingshall be as specified on manufacturer's shop drawings
·	For piping installed above a dropped ceiling, the open end[s] of the sampling pipe[s]shall penetrate the ceiling tile to act as an additional sampling point.
·	Pipes shall be suspended from ceiling slab-using hangers or clamp at intervals of nomore than 4 feet to ensure the stability of the piping and reduce the possibility of cracks and breaks at the joints.
·	All connections and joints shall be made with standard connections designed to be compatible with the pipe materials. All joints shall be secured according to standardpractices.
·	All joints shall be airtight to prevent air leakage or infiltration, which may adverselyaffect the desired venturi affect in the piping.
·	Provide all sampling point pipe caps with predrilled holes per manufacturer's shopdrawings.
·	The design program for the air sampling pipe network shall provide a balancedengineered system and ensure equal sensitivity at each sampling point.

4	**Installation of Smoke Detection System**
i.	The SDC Operator shall install the system in accordance with the manufacturer's recommendation.
ii.	Where false ceilings are available, the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.
iii.	The minimum internal diameter of the Capillary tube shall be 5mm, the maximum length of the capillary tube shall be 2m unless the manufacturer in consultation withthe engineer have specified otherwise.
iv.	The Capillary tube shall terminate at a ceiling Sampling Point specifically approved by the Client. The performance characteristics of the sampling points shall be taken into account during the system design.
v.	Air sampling piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.
5	**Commissioning test**
i.	Commissioning of the entire installation shall be done in the presence of the clientand/or its representative.
ii.	All necessary instrumentation, equipment, materials and labour shall be provided bythe SDC Operator.
iii.	The SDC Operator shall record all tests and system calibrations and a copy of theseresults shall be retained on site in the system Log Book.
3.6	**Functional test**
i.	Introduce Smoke into the Detector Assembly to provide a basic functional test.
ii.	Introduce smoke to the least favorable Sampling Point in each Sampling Pipe.Transport time is not to exceed as per manufacturer recommendation

Sr.	Description
	Access Control System
	Bidder to visit the SDC Site, check and study the existing installed Access ControlSystem for Phase 1 SDC. If existing system or any of its components are sufficient to cater to the future load, then only required components / equipment's to be proposed for the proposed new Server Room expansion area in compliance to below mentioned technical/functional requirements.

An access control system consisting of a central PC, intelligent controllers, proximity readers, power supplies, proximity cards, and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm, or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts.

1	**Access Control System**
	The Access Control System shall be modular and hot redundant in nature, and shall permit expansion of both capacity and functionality through addition of controllers,card readers and sensors.
2	**Operational Requirement**
	The access control system shall be a web based access control system whereby anycomputer can be used to operate the controller (or control panel) directly using a standard web browser program available freely. The controller shall be a black-box design with embedded software built-in, integrated with BMS including a web server program. The basic functions are:
·	Card access control
·	Alarm monitoring and handling procedures
·	Time Attendance data capture and post processing
3	**Technical Specification**
	Control panel with Power supply, IP on board.
·	Controller should be a microprocessor-based device conforming to UL 294/ EN 62368-1 / IEC 60950 / ERDA
·	Control Panel has to configure with minimum 6 numbers of doors.
·	It should feature a direct LAN/WAN connection to the controller bus structure in addition to Serial connections, all of which shall be designed for use incommunication with the ACS server.
·	It should have built in RDBMS database capable to store personnel particulars likename, Rank, Designation, department, card information and time zone.
·	It should be capable of reporting the following alarm conditions to the ACS fileserver:
	(i) Enclosure door tamper
	(ii) Primary power failure
	(iii) Low Battery Conditions
	(iv) Loss of Communications
	(v) All access control violations
·	Provision to integrate with Intruder alarm, Elevator Control, CCTV & DVR, Photo ID, Building Automation.
4	**Management Software for Access control system**

·	The system should have a simple, easy to use graphical user interface which is browser based, and all functions shall be accessible by use of either mouse or keyboard. Help text shall be provided for each screen function, and shall be sufficiently interactive that a user may access page help directly and be provided with explicit information relevant to the particular screen being displayed.
·	The software Navigation window should facilitate easy access to personnel details, remote controlling of controller operations and operating modes etc.
·	Should have provision to provide door wise access report for time monitoring of users.
·	Should have Global and local anti-pass back/anti-tailgate capability.
·	System must have provision of creation of data bank, easy retrieval of information and validity expiry warning.
·	The software shall seamlessly support and integrate with the smart cards and other access control hardware which is part of the total solution.
5	**Contact less Access Control Readers:**
·	Contact less smart card readers shall work on 13.56 MHz frequency, comply with ISO standard
·	All RF data transmission between the card and the reader shall be encrypted, using a secure algorithm and 64-bit authentication keys.
·	Typical contact less smart card read range shall be 2"– 3"
6	**Biometric Contactless Smart Card Readers:**
·	Fingerprint biometric authentication. Should provide to choose level of security with various combinations Card and fingerprint (Biometric).
·	The fingerprint reader should read fingerprint template(s) from a Smart Card and verify with a live finger placed on the fingerprint sensor, giving an audible and visual indication to indicate successful/unsuccessful authentication.
·	The reader should provide the following audiovisual indications:-
o	An audio transducer should provide various tone sequences to signify: access granted, access denied, power up and diagnostics.
o	A high-intensity light bar shall provide clear visual status (red/green/amber) that is visible even in bright sunlight.
·	Should be compact but rugged to withstand handling by multiple users. Verification time should be less than 10 sec.
·	May have separate fingerprint enrolment/programming facility to transfer fingerprint to smart card.
7	**Electro Magnetic Door Lock**
·	Should have holding force of min 600lbs.
·	Should me mountable on wooden/Glass doors.
·	Should have provision to be wired with Fire alarm.

Sr.	Description
	CCTV System
1	**General**
·	Specifications included in this section are indicative and considered as a minimum; component and software that shall be acquired at the time of implementing the project shall be the latest versions available in the market.
·	43-inch CCTV Monitor to be provided along with the system for Monitoring
2	**Camera**
·	1/2.8" progressive scan CMOS or better
·	1920 × 1080@30fps
·	2.8 mm/4 mm/6 mm fixed lens
·	Max. Resolution - 1920 × 1080
3	**Network Video Recorder**
·	16 channel NVR, with 2 SATA slots & compatible HDD for an ideal and flexible solution
·	Input- H.265/ H.265+/H.264/ H.264+/MPEG4 video formats, supports audio compressions Recording, Playback, Back-up, Network recording, and Networkplayback
·	Supports live view, storage, and playback of the connected camera
·	Storage capacity to store more than 120 days backup
·	HDMI and VGA independent outputs provided
·	Rated voltage: 220-240 VAC 50/60Hz.

Rodent Repellent

Sr.	Specification
	The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non- toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.
1	Configuration : Master console with necessary transducer and Cabling
2	Operating Frequency : Above 20 KHz (Variable)
3	Sound Output : 50 dB to 110 dB (Not audible to humans)
4	Power output : 800 mW per transducer
5	Power consumption : 15 W approximately
6	Power Supply : 230 V AC 50 Hz
7	Mounting : Wall / Table Mounting
8	The cabling for Rodent Repellent should properly routed in the false ceiling as well asfor false flooring.

END OF SECTION-4

SECTION-5

PROJECT EXPERIENCE

S. No	Item	Details
General Information		
1	Customer Name/Government Department	
2	Name of the Contact Person and Contact details for the Project	
Brief Description of scope of Project		
Size of the Project		
3	Contract Value of the Project (in crore) excluding taxes	
4	Contract Value of the Project (in crore) including taxes	
Project Details		
5	Name of the Project	
6	Start Date & End Date	
7	Current Status (work in progress in %, completed)	
8	Contract Tenure	
9	Type of Project	

END OF SECTION-5

SECTION – 6

<mark>PRICE BID SCHEDULE</mark>

<mark>(Price Bid format will be followed strictly as per client's tender)</mark>

Summary of Cost Components Table

S. No	Item	Schedule	TOTAL PRICE (Rs.) [including All Taxes out of pocket expenses and other charges etc)]
Cost of new Equipment/Products	New equipment/Products (Please give details in the A0 schedule defined in the RFP)	A0	
	Cost of any other items	A01 (Create schedule if needed)	
	Total new Equipment/Products Cost = Schedule (A0+A01)		
O&M Cost for 5 years	AMC & Warranty -Active and Passive, Non IT Components at SDC	A	
	Total O&M Cost for 5 years =Schedule (A)		
TOTAL PROJECT COST (in INR) = Total new Equipment/Products Cost + Total O&M Cost for 5 years			
(Gross Bid Value = Total new Equipment/Products Cost + Total O&M Cost for 5 years) in Words Rs.			

1. **Schedule A0**

i. Capital Cost Table- Schedule A0

a. Hardware (For Expansion BoM)

Sr.No.	Description	Qty	Make & Model	Unit Rate (INR)	Total Amount (INR) (A)	Tax (INR) (B)	Total (INR) (A+B)
4.	New Equipment 1						=x1
5.	New Equipment 2						=x2
6.	…….						
7.	New equipment n						=xn
	Total Cost for new equipment at SDC						**E1=Σ (xn1)**

b. Software Item (For Expansion BoM)

Sr.No.	Description	Qty	Make & Model	Unit Rate (INR)	Total Amount (INR) (A)	Tax (INR) (B)	Total (INR) (A+B)
4.	New Software 1						=x1
5.	New Software 2						=x2
6.	…….						
7.	New Software n						=xn
	Total Cost for new Software at SDC						**E2=Σ (xn1)**

c. Hardware (For Replacement of Existing items that will become EOS during the contract)

Sr.No.	Description	Qty	Make & Model	Unit Rate (INR)	Total Amount (INR) (A)	Tax (INR) (B)	Total (INR) (A+B)
4.	New Equipment 1						=x1
5.	New Equipment 2						=x2
6.	…….						

7.	New equipment n						=xn
	Total Cost for new equipment at SDC						**E3=Σ (xn1)**

Note: Bidder may replace existing items with items of similar or better configuration.

d. Software Item (For Replacement of Existing items that will become EOS during the contract)

Sr.No.	Description	Qty	Make & Model	Unit Rate (INR)	Total Amount (INR) (A)	Tax (INR) (B)	Total (INR) (A+B)
4.	New Software 1						=x1
5.	New Software 2						=x2
6.	…….						
7.	New Software n						=xn
	Total Cost for new Software at SDC						**E2=Σ (xn1)**

e. Add on Items (Scalability BOM)

Sr.No.	Description	Qty	Make & Model	Unit Rate (INR)	Total Amount (INR) (A)	Tax (INR) (B)	Total (INR) (A+B)
4.	Item 1						=x1
5.	Item 2						=x2
6.	…….						
7.	Item n						=xn
	Total Cost for Add On Items						**E2=Σ (xn1)**

ii. Operational cost (O&M) Table – Schedule A

a. **Operational Cost for all Hardware, Software and Non IT Equipment**

Note: bidders are required to enter separate line item for each Component mentioned in Expansion BoM as well as Existing BoM.

S. No	Item	Description	Annual Rate (A)	Annual Tax (B)	Total Annual Rate C=(A+B)	Total AMC cost for 5 years (=C*5)
IT Hardware						
1.	Hardware Item 1					
2.	Hardware Item 2					
3.	….					
4.	Hardware Item n					
IT Software						
5.	Software Item 1					
6.	Software Item 2					
7.	….					
8.	Software Item n					
Non IT						
9.	Non IT Item 1					
10.	Non IT Item 2					

11.	….					
12.	Non IT Item n					
OPEX (in INR) – Total Cost (incl. Support, Maintenance & Operations)						

Summary
Total AMC & Warranty (in INR) =
Total Cost for AMC & Warranty for entire Five Years i.e. Total AMC & Warranty in Words

b. Operational Cost of Add on Items (Scalability BOM)

S. No	Item	Description	Annual Rate (A)	Annuaal Tax (B)	Total Annual Rate C=(A+B)	Total AMC cost for 5 years (=C*5)
1.	Item 1					
2.	Item 2					
3.	….					
4.	Item n					

OPEX (in INR) – Total Cost (incl. Support, Maintenance & Operations)		

Note:

a. It is mandatory to provide breakup of all Taxes, Duties and Levies wherever applicable and/ or payable under the relevant column in the schedules. State shall take into account all Taxes, Duties & Levies for the purpose of Evaluation.

b. If there is a change in Taxes or other governmental levies are affecting customer as an importer or its OEM then the same will be passed on to the Purchaser. For this purpose, Supplier shall give detailed break-up of various duties, taxes and levies to the Purchaser.

c. ***The bidder will ensure that prices/cost for all the software licenses discovered during the bid process will be valid for entire period of contract and without any additional Operational & Maintenance Charges for the same.***

d. ***Licenses procured are perpetual in nature but support should be for 5 years.***

e. Server/ Network Racks required for EMS, other management solutions, Network would be brought by DCO along with its solution without any additional cost to thecustomer or ITI

f. **The quantities mentioned in the BoM are indicative and may change at the time of Order placement.**

g. Any changes in the layout which results leading to the changes in quantity and price will be borne by the DCO.

h. The bidder will ensure that prices/cost for all the software licenses discovered during the bid process will be valid for entire period of contract.

i. Additional licenses (if required) would be procured as per the same commercial or as mutually agreed between customer, ITI and bidder

j. All components/Licenses purchase from the selected bidder under customer from the day one shall be with the name of Client.

k. This Operational Support per year shall be for the entire components / items / infrastructure of SDC under the RFP / Contract including the Support personnel deployed for the project. Bidder should ensure that Manpower resources required for Operations and Maintenance of HP SDC project should comply as per the RFP. In case there are changes in technology, (such as addition or Up-gradation of Hardware, Software, Tools, equipments, active or passive) DCO needs to provide the resources with suitable technical competencies in line with project requirements without any additional charges as and when required.

l. **Please note**: Operational expenses during operation phase (such as Electricity, Diesel consumption {by DG-Set}, etc) will be paid by the Client to DCO as per the actual usage/ consumption as per the prevailing market price. DCO shall integrate the energy meter (for electricity) as well as diesel consumption reading of DG Set with the BMS infrastructure for ensuring automatic information update regarding actual consumption/usage. DCO shall have to pay

directly the electricity bills of HP SDC to the electricity department and the diesel vendor for diesel. However the Client shall reimburse based on theinformation available on the BMS infrastructure to the DCO. More ever the other cost associated with DG Set running shall be born by the bidder itself.

END OF SECTION-6

SECTION-7

MANUFACTURER'S AUTHORISATION FORM

As per client's tender.

Note: I. This letter of authorization should be on the letter head of the manufacturing firm and should be signed by a person competent and having the Authorization letter / Board Resolution to legally bind the manufacturer.

2. Original letter may be sent.

END OF SECTION-7

SECTION-8

INTEGRITY PACT

THIS Integrity Pact is made on…………………day of......................... 22.

BETWEEN:

ITI Limited having its Registered & Corporate Office at ITI Bhavan, Dooravaninagar, Bangalore – 560 016 and established under the Ministry of Communications, Government of India (hereinafter called the Principal), which term shall unless excluded by or is repugnant to the context, be deemed to include its Chairman & Managing Director, Directors, Officers or any of them specified by the Chairman & Managing Director in this behalf and shall also include its successors and assigns) ON THE ONE PART

AND:

………………………………………………….. represented by .... Chief Executive Officer (hereinafter called the Contractor(s), which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the contractor ON THE SECOND PART.

Preamble

WHEREAS the Principal intends to award, under laid down organizational procedures, contract for ……………………………………………. of ITI Limited. The Principal, values full compliance with all relevant laws of the land, regulations, economic use of resources and of fairness/ transparency in its relations with its Contractor(s).

In order to achieve these goals, the Principal has appointed an Independent External Monitor (IEM), who will **monitor** the tender process and the execution of the contract for compliance with the principles as mentioned herein this agreement.

WHEREAS, to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact the terms and conditions of which shall also be read as integral part and parcel of the Tender Documents and contract between the parties.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL COVENANTS STIPULATED IN THIS PACT THE PARTIES HEREBY AGREE AS FOLLOWS AND THIS PACT WITHNESSETH AS UNDER:

SECTION 1 – COMMITMENTS OF THE PRINCIPAL

The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a.   No employee of the Principal, personally or through family members, will in connection with the tender for or the execution of the contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the personal is not legally entitled to.

b.   The Principal will, during the tender process treat all bidder(s) with equity and reason. The Principal 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 tender process or the contract execution.

c.   The Principal will exclude from the process all known prejudiced persons.

If the Principal obtains information on the conduct of any of its employee, which is a criminal offence under IPC/PC Actor if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary action as per its internal laid down Rules/ Regulations.

SECTION 2 – COMMITMENTS OF THE BIDDER/CONTRACTOR

The Contractor(s) commits himself to take all measures necessary to prevent corruption. He commits himself observe the following principles during the participation in the tender process and during the execution of the contract.

a.   The contractor(s) will not, directly or through any other person or firm offer, promise or give to any of the Principal'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 of any kind whatsoever during the tender process or during the execution of the contract.

b.   The contractor(s) will not enter with other contractors 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 contractor(s) will not commit any offence under IPC/PC Act, further the contractor(s) will not use improperly, for purposes of competition of personal

gain, or pass onto others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d.   The Contractor(s) of foreign original 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.

e.   The Contractor(s) will, when presenting the bid, disclose any and all payments made, are committed to or intend to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f.   The Contractor(s) will not bring any outside influence and Govt bodies directly or indirectly on the bidding process in furtherance to his bid.

g.   The Contractor(s) will not instigate third persons to commit offences outlined above or to be an accessory to such offences.

SECTION 3 – DISQUALIFICATION FROM TENDER PROCESS & EXCLUSION FROM FUTURE CONTRACTS

If the Contractor(s), during tender process or before the award of the contract or during execution has committed a transgression in violation of Section 2, above or in any other form such as to put his reliability or credibility in question the Principal is entitled to disqualify Contractor(s) from the tender process.

If the Contractor(s), has committed a transgression through a violation of Section 2 of the above, such as to put his reliability or credibility into question, the Principal shall be entitled exclude including blacklisting for future contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the Principal taking into consideration the full facts and circumstances of each case, particularly taking into account the number of transgression, the position of the transgressor within the company hierarchy of the Contractor(s) and the amount of the damage. The exclusion will be imposed for a period of minimum one year.

The Contractor(s) with its free consent and without any influence agrees and undertakes to respect and uphold the Principal's absolute right to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground including the lack of any hearing before the decision to resort to such exclusion is taken. The undertaking is given freely and after obtaining independent legal advice.

A transgression is considered to have occurred if the Principal after due consideration of the available evidence concludes that on the basis of facts available there are no material doubts.

The decision of the Principal to the effect that breach of the provisions of this Integrity Pact has been committed by the Bidder(s)/ Contractor(s) shall be final and binding on the Bidder(s)/ Contractor(s), however the Bidder(s)/ Contractor(s) can approach IEM(s) appointed for the purpose of this Pact.

On occurrence of any sanctions/ disqualifications etc arising out from violation of integrity pact Bidder(s)/ Contractor(s) shall not entitled for any compensation on this account.

subject to full satisfaction of the Principal, the exclusion of the Contractor(s) could be revoked by the Principal if the Contractor(s) can prove that he has restored/ recouped the damage caused by him and has installed a suitable corruption preventative system in his organization.

SECTION 4 – PREVIOUS TRANSGRESSION

The Contractor(s) declares that no previous transgression occurred in the last 3 years immediately before signing of this Integrity Pact with any other company in any country conforming to the anti-corruption/ transparency International (TI) approach or with any other Public Sector Enterprises/ Undertaking in India of any Government Department in India that could justify his exclusion from the tender process.

If the Contractor(s) makes incorrect statement on this subject, he can be disqualified from the tender process or action for his exclusion can be taken as mentioned under Section-3 of the above for transgressions of Section-2 of the above and shall be liable for compensation for damages as per Section- 5 of this Pact.

SECTION 5 – COMPENSATION FOR DAMAGE

If the Principal has disqualified the Bidder(s)/Contractor(s) from the tender process prior to the award according to Section 3 the Principal is entitled to forfeit the Earnest Money Deposit/Bid Security/ or demand and recover the damages equitant to Earnest Money Deposit/Bid Security apart from any other legal that may have accrued to the Principal.

In addition to 5.1 above the Principal shall be entitled to take recourse to the relevant provision of the contract related to termination of Contract due to Contractor default. In such case, the Principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor or demand and recover liquidate and all damages as per the provisions of the contract agreement against termination.

SECTION 6 – EQUAL TREATMENT OF ALL BIDDERS/CONTRACTORS

The Principal will enter into Integrity Pact on all identical terms with all bidders and contractors for identical cases.

The Bidder(s)/Contractor(s) undertakes to get this Pact signed by its sub- contractor(s)/sub-vendor(s)/associate(s), if any, and to submit the same to the Principal along with the tender document/contract before signing the contract. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the provisions laid down in the Integrity Pact Agreement by any of its sub-contractors/sub- vendors/associates.

The Principal will disqualify from the tender process all bidders who do not sign this Integrity Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATING BIDDER(S)/ CONTRACTOR(S)

7.1 If the Principal receives any information of conduct of a Contractor(s) or sub- contractor/sub-vendor/associates of the Contractor(s) which constitutes corruption or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer of the Principal for appropriate action.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR(S)

The Principal appoints competent and credible Independent External Monitor(s) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extend the parties comply with the obligations under thispact.

The Monitor is not subject to any instructions by the representatives of the parties and performs his functions neutrally and independently. He will report to the Chairman and Managing Director of the Principal.

The Contractor(s) accepts that the Monitor has the right to access without restriction to all product documentation of the Principal including that provided by the Contractor(s). The Bidder(s)/Contractor(s) will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The Monitor is under contractual obligation to treat the information and documents Contractor(s) with confidentiality.

8 .4 The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meeting could have an impact on the contractual relations between the Principal and the Contractor(s). As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal 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 specific manner, refrain from action or tolerate action.

The Monitor will submit a written report to the Chairman & Managing Director of the Principal within a reasonable time from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.

If the Monitor has reported to the Chairman & Managing Director of the Principal a substantiated suspicion of an offence under relevant IPC/PC Act, and the Chairman & Managing Director of the Principal 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.

The word **'Monitor'** would include both singular and plural.

Any changes to the same as required / desired by statutory authorities is applicable.

SECTION 9 – FACILITATION OF INVESTIGATION

9.1 In case of any allegation of violation of any provisions of this Pact or payment of commission, the Principal or its agencies shall be entitled to examine all the documents including the Books of Accounts of the Bidder(s)/Contractor(s) and the Bidder(s)/Contractor(s) shall provide necessary information and documents in English and shall extend all help to the Principal for the purpose of verification of the documents.

SECTION 10 – LAW AND JURISDICTION

The Pact is subject to the Law as applicable in Indian Territory. The place of performance and jurisdiction shall the seat of the Principal.

The actions stipulated in this Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

SECTION 11 – PACT DURATION

This Pact begins when both the parties have legally signed it. It expires after 12 months on completion of the warranty/guarantee period of the project / work awarded, to the fullest satisfaction of the Principal.

If the Contractor(s) is unsuccessful, the Pact will automatically become invalid after three months on evidence of failure on the part of the Contractor(s).

If any claim is lodged/made during the validity of the Pact, the same shall be binding and continue to be valid despite the lapse of the Pact unless it is discharged/determined by the Chairman and Managing Director of the Principal.

SECTION 12 – OTHER PROVISIONS

This pact is subject to Indian Law, place of performance and jurisdiction is the Registered& Corporate Office of the Principal at Bengaluru.

Changes and supplements as well as termination notices need to be made in writing by boththe parties. Side agreements have not been made.

If the Contractor(s) or a partnership, the pact must be signed by all consortium members and partners.

Should one or several provisions of this pact turn out to be invalid, the remainder of this pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

Any disputes/ difference arising between the parties with regard to term of this Pact, any action taken by the Principal in accordance with this Pact or interpretation thereof shall notbe subject to any Arbitration.

12.5 The action stipulates in this Integrity Pact are without prejudice to any other legal action thatmay follow in accordance with the provisions of the extant law in force relating to any civilor criminal proceedings.

In witness whereof the parties have signed and executed this Pact at the place and date firstdone mentioned in the presence of the witnesses:

For PRINCIPAL   For CONTRACTOR(S)

………………………………
……(Name & Designation)
Designation)

………………………………
(Name &

Witness   Witness

1)   ……………………………1)…………………………………………...

2)   …………………………….   2)……………………………………...

END OF SECTION-8

SECTION-09

NO-CONVICTION CERTIFICATE

[To be submitted on the Letterhead of the Bidder]

Offer No.: _____   Date: _____

To
[Head of Department]
Telecommunications Consultants India Limited,
ITI Bhawan, Greater Kailash-I,
New Delhi-110 048 (INDIA)

Sub: Self Declaration of not been blacklisted for [EOI No.] dated [EOI date]

Dear Sir,

This is to notify you that our Firm /Company/ Organization <p**rovide Name of the Firm/ Company/Organization>** intends to submit a proposal in response to [EOI No.] dated [EOI date] for [EOI Name].

In accordance with the above, we declare that:

a. We are not involved in any major litigation that may have an impact of affecting or compromising thedelivery of goods / services as required under this [EOI No] dated [EOI date].

b. We are neither banned/ debarred/ blacklisted/ put on holiday list nor action for banning / debarment /blacklisting / holiday listing has been initiated by any Central/ State Government/ agency of Central/ State Government of India or any other country in the world/ Public Sector Undertaking/ any Regulatory Authorities in India or any other country in the world for any kind of fraudulent activitieson any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercivepractice, undesirable practice or restrictive practice as on date of submission of the Bid.

Yours sincerely,

(Signature of the Authorized signatory of the Bidding

Organisation)Name:

Designation:

Contact details (including E-mail):

Business Address:

Date:

Inventory & Expansion BOM

Note: (1) Equipment becoming obsolete during the currency of contract shall be replaced by the bidder as and when the equipment is declared obsolete by the OEM.

(2) If bidder proposes replacement of any End of Life/End of Service Hardware, the bidder shall be responsible for all configuration, application, data and database migration to the new hardware. Any such application migrated to new platform shall be made up and running by the bidder without any loss of functionality and data. The bidder shall demonstrate the migration to proposed environment to CUSTOMER through a PoC during Technical Evaluation of bids.

(3) Further, in case bidder is proposing replacement of End of Life/End of Service Servers, the bidder shall ensure that the configuration of proposed servers such as number of processor cores, RAM and Hard Disk size etc. and performance of these components should be equal or higher than that of existing Servers. The bidder shall also be responsible for providing additional OS/Database licenses (if required) on account of difference in server configuration at no additional cost to the client.

(4) Any Rack or Blade server proposed to be replaced shall be replaced by the bidder with servers having minimum specifications mentioned in the RFP, except the following rack servers, which may be replaced with rack servers of equivalent or better specifications:

      1. Staging server
      2. Non IT Rack servers
      3. HPPCL Rack server

(5) It may further be noted that rack servers shall be replaced with rack servers and blade servers with blade servers. In case bidder proposes to replace blade servers with rack servers then the power consumption and 42U rack space occupied shall not exceed that of the existing blade servers.

(6) Bill of Material items mentioned for HPPCL shall be quoted separately and may not be merged with SDC, eDistrict items.

Existing BoM
6.1 Existing Hardware Inventory – IT (SDC)

SN	Component	Make	Model	Specifications	Count
1	Firewall	Cisco	cisco_asa_5585_ssp20	ASA 5585-X Chassis with SSP20 8GE 2 SFP 2 Mgt 1 AC 3DES/AES, ASA 5585-X Security Services Processor-20 with 8GE, AnyConnect Essentials VPN License 5k users - ASA 5585-X	2

2	OOB Switch	Cisco	WS-C2960X-48LPS-L	24 Gigabit Ethernet ports with line-rate forwarding performance, 4 fixed 1 Gigabit	6
3				Ethernet Small Form-Factor Pluggable (SFP) uplinks or 2 fixed 10 Gigabit Ethernet SFP+ uplinks, PoE+ support with a power budget of up to 740W and Perpetual PoE, RJ-45 or USB console access, Layer 3 features with routed access, Security with 802.1X	
3	Rack Servers	Cisco	UCSC-C220-M3	UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/ rail kit 2 * Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz, 2200 Mhz, 10 Core(s) 2 * Intel(R) C600/X79 series chipset USB2 Enhanced Host Controller 2 * Emulex LPe 12002 Dual Port 8Gb Fibre Channel HBA 2 * Broadcom	6

				5709 Dual Port 1Gb w/TOE iSCSI	
				4 * 16GB DDR3-1600-MHz	
				RDIMM/PC3-12800/dual rank/1.35v	
				2 * 1TB 6Gb SATA 7.2K RPM SFF HDD/hot plug/drive sled mounted	
4	Rack Servers	Cisco	UCSC-C420-M3	UCS C420 M3 w/o CPU mem HDD PCIe PSU rail kit, 2 * Intel X520 Dual Port 10Gb SFP+ Adapter, 2 * Emulex LPe 12002 Dual Port 8Gb Fibre Channel HBA 1TB RAM – DDR3-1600-MHz RDIMM/PC3-12800/dual rank 4 * 300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted 4* Intel Xeon E5-4650), No of CPU (8 core each), 2.70GHz	5

5	Rack Server - Staging	Cisco	Cisco UCSC-C420-M3	UCS C420 M3 w/o CPU mem HDD PCIe PSU rail kit 1 * Intel X520 Dual Port 10Gb SFP+ Adapter-2 Nos)	1
				1 * Emulex LPe 12002 Dual Port 8Gb Fibre Channel HBA 128 GB RAM – DDR3-1600-MHz RDIMM/PC3-12800/dual rank 2 * 300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted 2 * Intel Xeon E5-4650), No of CPU (8 core each), 2.70 GHz	

| 6 | Router | Cisco | cisco_asr1002x | ASR1002-X 5G VPN Bundle K9 AES license

IPSEC License for ASR1002-X 4G crypto BW

Cisco ASR 1000 Advanced Enterprise Services License

Cisco 2-Port Gigabit Ethernet Shared Port Adapter

1000BASE-SX SFP transceiver module MMF 850nm DOM

8-port Channelized T1/E1 to DS0 Shared Port Adapter

2 * 1000BASE-SX SFP transceiver | 2 |

				module MMF 850nm DOM 4 * 1000BASE-T SFP (NEBS 3 ESD) Cisco ASR1002-X 4GB DRAM	
7	SAN Switch	Cisco	cisco_mds_9513	Cisco MDS 9506 Base Config: Chassis,2 Sup-2A, 2 1.9K AC PS 1 * Cisco MDS 9000 Family 32-port Advanced FC Module + 32 2/4/8-Gbps SW SFP+, with lic 1 * Cisco MDS 9000 Family 48-port Advanced FC Module + 48 2/4/8-Gbps SW SFP+, with lic 80 * 50/125 LC/LC PLN 10M 2f round SB 10gig OM3 MDS-9500 Entrprs Pkg Lic for 1 MDS9500 switch	2
8	UCSM-Fabric Interconnect	Cisco	UCS 6296UP	UCS 6296UP 2RU Fabric Int/No PSU/48 UP, UCS 6296UP Chassis Accessory Kit UCS 6200 16-port Expansion module/16 UP/ 8p LIC 24 * 8 Gbps	2

				Fibre Channel SW SFP+, LC	
				24 * 10GBASE-SR SFP Module	
				28 * Active Twinax cable assembly, 7m	
				22 * UCS 6200 Series ONLY Fabric Int 1PORT 1/10GE/FC-port license	
				4* UCS 6296UP Fan Module	
				UCS 6200 16-port Expansion module/16 UP/ 8p LIC	
				KVM local IO cable for UCS servers console port	
9	Storage	Hitachi	Hitachi HUS VM	HUS / HUS VM File Module SMU	1
				4 * 10G 850nm XFP	
				2 * 50/125 LC/LC PLN 1M 2f round SB 10gig OM3	
				8 * 50/125 LC/LC PLN 3M 2f round SB 10gig OM3	
				HUS / HUS VM File Module M1 SW Lic - 70 TB	
				HUS VM Cache	

				Flash Memory Module (supports 160GB)	
				4 * HUS VM B/E I/O Module	
				7 * HUS VM Drive Box (SFF)	
				5 * HUS VM 200GB SAS SSD SFF for DBS-Base	
				141 * HUS VM 300GB SAS 15K RPM HDD SFF for CBSS/DBS-Base	
				17 * HUS VM 3TB SAS 7.2K RPM HDD LFF for DBX-Base	
				8 * HUS VM 8GB Cache Module	
				8 * HUS VM 4x8Gbps FC Interface Adapter	
				32 * 50/125 LC/LC PLN 25M 2f round SB 10gig OM3	
				Remote Replication Base License (20TB)	
				Local Replication 20TB Block	

				License RAID Level (1, 5, 6)	
10	Storage	Hitachi	Hitachi VSP 1000	260TB usable space 4 * BEDs, 2 * VSD, 2 * Cache Board (256 GB), 2 * BKM (Battery Backup module), 2 * VSP Rack with disk enclosures (HDU) and required PDU, 32 * Fibre Ports (2 x 16 ports - 16+16=32 ports), 4 * 3.2TB Flash, 48 * 6TB SAS 7.2 K LFF, 48 * 1.8TB SAS SFF, Dynamic Provisioning, Dynamic Tiering, Capacity, and all necessary Licenses, Cables and all other accessories which is required to connect required components with existing SAN, and SAN Switch, RAID Level 1, 5, 6	1
11	Router-Telco	Juniper	J4350	4 * fixed GE	1

				LAN ports, 4 PIM slots, and 2 EPIM/PIM slots	
				1 GB DRAM, expandable to 2 GB DRAM	
12	Tape Library with LTO-6 Drives	Quantum	Quantum scaler i500	23U Base Library, 225 activated slots 12 * LTO-6 Tape Drive Module, Scalar Key Manager-Enabled, 8Gb native Fibre Channel, 9U Expansion Module, zero activated slots, 46-slot License Key, 12 * Fibre Channel Interface Cable, OM3 optical multimode 50 micron, LC-to-LC, 24.5 ft (7.5 m) 500 * LTO Ultrium 6 (LTO-6). 2 * Cleaning cartridge	1
13	IPS	Radware	Product -DP-1016-NL-D-Q	Defense-Pro 1016 - OnDemand Switch 2S2 - 4*SFP - 12*GE - 6GB, Memory - 1Gbps inspection throughput - Dual AC Power Supply and String Match	2

				Engine - 2U - RoHS. Includes Signature Protections, Behavioral Protections and BWM. With signature Update	
14	IPS Manager	Radware	Radware Apsolute vision	Q9400 Intel Quad 2.6Ghz 2 Gigabit Ethernet Ports (Copper) USB Port Front Panel	1
15	Access Switch (48 Ports)	Cisco	Cisco N6K-C6001-64P	Nexus 6001 1RU switch fixed 48p of 10GSFP+ and 4p QSFP+ 3 * Nexus 6001 Fan for Front to Back airflow, 2 * Nexus 1100W PlatinumPS Forward airflow, 16 * 1000BASE-T SFP 32 * 10GBASE-SR SFP Module, Promo Layer 3 License for Nexus 6001	6
16	Access Switch (24 Ports)	Cisco	Cisco N6K-C6001-64P	Nexus 6001 1RU switch fixed 48p of 10GSFP+ and 4p QSFP+ 3 * Nexus 6001 Fan for Front to Back	3

				airflow, 2 * Nexus 1100W PlatinumPS Forward airflow, 12 * 1000BASE-T SFP 12 * 10GBASE-SR SFP Module, Promo Layer 3 License for Nexus 6001	
17	Blade Chassis	Cisco	5108	UCS 5108 Blade Svr AC Chassis/0 PSU/8 fans/0 fabric extender, UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)), UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)), Accessory kit for UCS 5108 Blade Server Chassis, 4 * Fan module for UCS 5108, 4 * Blade slot blanking panel for UCS 5108/single slot	6

18	Blade Server	Cisco	UCSB-B420-M3	UCS B420 M3 Blade Server w/o CPU, memory, HDD, mLOM, 2 * 2.70 GHz E5-4650 130W 8C/20MB Cache/DDR3 1600MHz ==16 * 8 GB== DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v 2 * 300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted Cisco UCS VIC 1280 dual 40Gb capable Virtual Interface Card Cisco UCS VIC 1240 modular LOM for M3 blade servers	12
19	Core Switch	Cisco	cisco_nexus_7018	18 Slot Chassis No Power Supplies Fans Included, Nexus 7K USB Flash Memory - 8GB (Log Flash) Nexus 7000 LAN Enterprise License (L3 protocols) Nexus 7000 - Supervisor 2 Enhanced includes 8GB USB Flash	2

				Nexus 7K USB Flash Memory - 8GB (Log Flash)	
				Nexus 7000 - Supervisor 2 Enhanced Includes 8GB USB Flash	
				2 * Nexus 7000 - 18 Slot Fan	
				18 * 1000BASE-SX SFP transceiver module MMF 850nm DOM	
				24 * 1000BASE-T SFP	
				36 * Active Twinax cable assembly 10m	
				Nexus 7000 F2-Series 48 Port 1/10G (SFP+) Enhanced	
				24 * 1000BASE-SX SFP transceiver module MMF 850nm DOM	
				Nexus 7000 F2-Series 48 Port 1/10G (SFP+) Enhanced	
				24 * 1000BASE-T SFP	
				5 * Nexus 7000 - 18 Slot Chassis - 110Gbps/Slot Fabric Module	
				2 * Nexus 7000 - 7.5KW AC	

				Power Supply Module	
20	SIEM	Trustwave	TS 500 Siem 3	12 TB storage within the appliance	1

Note: The two storages mentioned at point 9 and 10 of above table, shall be replaced by the bidder with new proposed storage with latest specifications.

Further, bidder shall be responsible for any Data/VM Migration from existing infrastructure to new infrastructure, if required, with minimal disruption. Any migration shall be done during Scheduled Maintenance Window approved by CUSTOMER.

6.2 Existing Software Inventory (SDC)

SN	Description	Make/OEM	Qty
1	Arcserve Backup Software	Arcserve	100 online agents
2	MS SQL Enterprise edition	Microsoft	20
3	Device CAL - Microsoft	Microsoft	30
4	Microsoft Windows Server Datacenter 2012R2 - 2 Proc	Microsoft	25
5	Servers Virtualization software (hypervisor)	Microsoft	18
6	Red Hat Linux Server Enterprise edition	RedHat	4
7	Trend Micro Security Suite	TrendMicro	100
8	TrendMicro Deep Security	TrendMicro	20
9	Websense Data Security Suite	WebSense DLP	250
10	Microsoft System Center DataCenter	Microsoft	25
11	Building Management System R430.1 (BMS Solution)	Honeywell	1
12	Visitor Management Software (Visman)	Honeywell	1
13	SiS Pre Ed 1 OSI Migration SW E-LTU(H7W94AAE)	MicroFocus	56
14	SiS Pre Ed OSI Mig Comp SW E-LTU(H7X14AAE)	MicroFocus	44
15	Ops Brdge Rep Ad 50 OBR Nds SW E-LTU(TJ756AAE)	MicroFocus	1
16	Network Node Manager i Ultimate Edition 50 Node Pack for 50+ Nodes Software E-LTU (A7Z73AAE)	MicroFocus	1
17	Network Node Manager i Points iSPI 100 Point Pack for 100 or more Points to NNMi Ultimate Edition for Migration Software E-LTU (A8A65AAE)	MicroFocus	2
18	UCMDB 10.00+ Foundation including Federation and Topology Entitlement Software E-LTU (TF235AAE)	MicroFocus	1
19	CloudSystem Enterprise Starter Suite Software E-LTU (TJ679AAE)	MicroFocus	1
20	OMi Evt Mgmt Foundation E-LTU(TA188AAE)	MicroFocus	1
21	Operations OS Inst Adv SW E-LTU(TB056AAE)	MicroFocus	20
22	Ops SPI Oracle DB In A SW E-LTU(TB059AAE)	MicroFocus	5
23	Ops SPI SQL Sv In A SW E-LTU(TB062AAE)	MicroFocus	5
24	Ops Mgr Windows Basic Suite SW E-LTU(TB681AAE)	MicroFocus	1
25	Service Manager Enterprise Suite with Connect-It Connectors and Knowledge Management Concurrent User Software E-LTU (TD741AAE)	MicroFocus	5

SN	Component	Make	Model	Count
26	UD OS Instance SW E-LTU(TF210AAE)	MicroFocus		140
27	Asset Mgr Ent Ste CC User SW E-LTU (TF283AAE)	MicroFocus		5
28	ART Service Manager Course (TJ641AAE)	MicroFocus		1
29	ART Asset Management Course (TJ643AAE)	MicroFocus		1
30	ART Universal Configuration Management Database Course (TJ649AAE)	MicroFocus		1
31	ART Operations Manager i Course (TJ652AAE)	MicroFocus		1
32	ART Network Node Manager i Series Course (TJ660AAE)	MicroFocus		1

6.3 Existing Hardware Inventory – Non-IT (SDC)

SN	Component	Make	Model	Count
1	Rack Server	IBM	System x3650 M4	2
2	UMG	Avocent	UMG 2000	1
3	**Civil & Interior Including:** > Brick work > Cement Concrete Work > Cutting and chipping of existing floors > Masonry works > Hardware and Metals > Glazing > False Flooring > False Ceiling > Diesel Storage Tank > Furniture & fixture > Partitioning > Doors and Locking > Painting > Fire proofing all surfaces > Water proofing > Insulating	Civil	NA	lumpsum
4	CAC Intelligent Timer	Daikin	NA	3
5	Split AC	Daikin	REL60PRV16	15
6	Split AC ODU	Daikin	REL60PRV16	15
7	BMS Desktop (with Monitor, Keyboard & Mouse)	Dell	T17M	3
8	AC Distribution Box	Electrical	NA	2
9	**Electrical items including:** > Electrical Cabling (Entire SDC area including all utility components, Power Socket with Switches, Earthing, Lightening & Fixture, motion detectors, main Electric Panel, MCBs	Electrical	NA	lumpsum
10	Raw power distribution box	Electrical	NA	2
11	Floor Power Distribution Unit	Electrical	NA	2
12	Light Distribution Box	Electrical	NA	2
13	LT Panel-SDC Electrical room	Electrical	NA	1
14	UPS Distribution Box	Electrical	NA	2

15	BMS UPS	Emerson / Vertiv	20 KVA	2
16	DC UPS	Emerson / Vertiv	APM 180KVA	2
17	Power Distribution Unit	Emerson / Vertiv	EP-ETR16NOXS30	54
18	Precision AC ODU	Emerson / Vertiv	LSF 52	9
19	Precision AC with accessories	Emerson / Vertiv	CRV 20RA	9
20	Battery Bank 20 KVA	Excide	SMF-65Ah	68
21	Chair	Geeken	GA505 Office Chair	20
22	Almirah	Godrej	NA	4
23	Media storage	Godrej	NA	2
24	Sofa	Godrej	Vegas	2
25	Table	Godrej	Claster-3	8
26	Camera - PTZ	Hikvision	DS-2AE7168	1
27	Actuator Assembly	Honeywell	890191	2
28	Amplifier	Honeywell	LBB 1990	1
29	Bio Metric Cards Reader	Honeywell	RKLB 57	1
30	BMS LAN Switch 24 P	Honeywell	Cisco SF 300 24p	1
31	BMS Panel - Alarm	Honeywell	AD-ESF1	1
32	BMS Panel - DDC	Honeywell	CP-IPC	2
33	BMS Panel - Fire Alarm	Honeywell	XLS3000	1
34	BMS Panel - GAS Release	Honeywell	RE-120GR	2
35	BMS Panel - Rodent	Honeywell	JE-1Z12	1
36	BMS Panel - VESDA	Honeywell	Faast 8100	1
37	BMS Panel - WLD	Honeywell	JE-3523	1
38	BMS Sensor - smoke	Honeywell	TC806B1076	35
39	BMS Speaker	Honeywell	LBD 8352	12
40	BMS Transducer	Honeywell	NA	10
41	Call Point	Honeywell	S464G1007	3
42	Camera - Dome	Honeywell	CADC600PIV-V	17
43	Cards Reader	Honeywell	R10 6100C	10
44	Control Module	Honeywell	NA	15
45	Monitor Module	Honeywell	NA	3
46	Desk MIC	Honeywell	LBD 1956	1
47	Digital Video Recorder	Honeywell	Capture 16 Port	2
48	Dome CAMERA Power Supplies (12 v)	Honeywell	12v	17
49	Fire Alarm panel battery (12 v)	Honeywell	12v	2
50	Fire Extinguisher	Honeywell	10 Nos CO2 & 1 ABC type	11
51	Fire Suppression cylinder	Honeywell	NOVEC1230	4
52	Gas Abort Switch	Honeywell	RE-716MY	2
53	Gas Release Switch	Honeywell	RE-716MG	2
54	Hooter	Honeywell	SYS/HS	3
55	Joystick	Honeywell	DS 1003KI	1
56	LED Monitor	Honeywell	42" LED Monitor	2
57	Magnetic Door Locks	Honeywell	UL275-SL	11
58	Panic Bar	Honeywell	DPB30-36	1
59	PTZ CAMERA Power Supplies (24 v)	Honeywell	24v	2
60	Push Button	Honeywell	NA	9
61	Response Indicator	Honeywell	NA	16

62	RTU with enclosure	Honeywell	NA	10
63	Sprinkler	Honeywell	NA	6
64	Tema Server	Honeywell	TS2	2
65	Temp & RH Sensor	Honeywell	RH100B03K	4
66	WLD Detection Sensor	Honeywell	NA	4
67	BMS - Visitor software camera	Logitech	2.0	1
68	Racks (Network & Servers)	MTS Infonet-42U	42U	16
69	Data cabling for complete DC including NOC, BMS, Non-IT etc.	Passve Cabeling	NA	lumpsum
70	LED Lights	Philips	NA	53
71	Tube Lights	Philips	NA	15
72	Battery Bank 180 KVA	Rocket	ESG-300, 2v	480
73	Camera - PTZ	Samsung	Songc M35	1
74	Stabilizer for 2 Tn AC	V-Guard	VG 500	15
75	Servo Voltage Stabilizer (600KVA) installed in Transformer room	Selvon	Selvon 600KVA	2

6.4 Existing E-District Project Hardware & Software

Sr. No	Device	Make	Model	Count
1	Blade Servers	Cisco	CISCO UCSB-B200-M3	9
2	Rack Servers	Cisco	CISCO UCSC-C420-M3	3
3	Blade Server FI	Cisco	CISCO UCS 6248UP Fiber Interconnect	4
4	Blade Chassis	Cisco	CISCO UCS 5108 Chassis	3
5	Load Balancer	Array	Array APV 10600	2
6	KVM Switch	Avocent	Avocent 8SV1000-106	3
7	KVM Display	Avocent	AP17KMM-106(LCD)	3
8	OS License	Microsoft	Microsoft Windows Server 2012R2	12

6.5 Existing HPPCL Project Hardware & Software

Sr. No	Device	Make	Model Name	Count
1	Blade Chassis	HP	HP C-7000	5
2	Blade Server	HP	HP BL 860 c	20
3	Rack Server	HP	HP DL180 G6	1
4	Tape Library	HP	HP MSL 4048	1
5	Blade Server	HP	HP BL 460 CG7	12
6	Blade Server	HP	HP BL 870 C	2
7	Blade Server	HP	HP BL 860 C	1
8	Rack 42 U, with PDU	APC	NA	5
9	Router	Juniper	Juniper SRX550M	1
10	Core Switch	Juniper	Juniper EX9208	1
11	Access Switch	Juniper	Juniper EX4200-48T	2
12	Access Switch	Juniper	Juniper SRX550M	1

13	Router	Juniper	Juniper EX4200-48T	1
14	Spam Filter	Barracuda	Barracuda Spam Filter 300 with subscription Lic	1
15	HP SAN Switch	HP	Entitlement Certificate	2
16	SAN Storage	HP	HP EVA P6000	1
17	HP c-Class FIO	HP	Entitlement Certificate for 16 Server License	3
18	HP-Ux 11iv3 BOE Integrity 2Skt/4Core PSL LTU	HP	License Entitlement Certificate, Product Quantity: 4	5
19	HP-Ux 11iv3 BOE Integrity 2Skt/4Core PSL LTU	HP	License Entitlement Certificate, Product Quantity: 2	15
20	HP Serviceguard NFS toolkit	HP	Codeword for software	7
21	HP Serviceguard Extension for SAP	HP	Codeword for software	7
22	PSL HP Serviceguard	HP	Codeword for software	7
23	HP Enterprise Cluster Master Toolkit	HP	Codeword for software	7
24	PSL HP Integrity VM	HP	Codeword for software	2
25	HP Online JFS for Veritas File System 5.1 SP1 Bundle	HP	Codeword for software	2
26	HP C/aC ++ Developer's Bundle	HP	Codeword for software	1
27	HP Data Protector 9.03	HP	HP Data Protector 1 Drive Extension UNIX/NAS/SAN E-LTU	2
			HP Data Protector On-line Backup for UNIX E-LTU	11
			HP Data Protector Starter Pack for Windows eMedia /eLTU	1
			HP Data Protector On-line Backup for Windows LTU	2
28	HPVM 6.0	HP	HPVM 6.0	1
29	Service Guard Cluster 11.20	HP	Service Guard Cluster 11.20	1
30	Number Licence(s) for MS Windows Server Ent 2008 R2	Microsoft	MS Windows Server Ent 2008 R2	8
31	Number Licence(s) for MS Windows Server Std 2008 R2	Microsoft	MS Windows Server Std 2008 R2	4
32	HP-UX administrator resources for O&M of above mentioned HW/SW and coordination with SAP-ERP application team to enable them to work on the machines	NA	NA	2
33	MS windows Server Datacenter Latest edition and Upgradation of Microsoft Exchange 2010 Mail Server to Microsoft Exchange 2016 (with clustering) with five years of updates & upgrades / equivalent Open Source software (wherever feasible)	Microsoft/ Open Source	Microsoft or open source	500 users

6.6 Servers Inventory – IT - SDC (to be covered under AMC from 25-Dec-2024 onwards)

Sr. No	Device	Make	Model Name	Count
1	Blade Servers	Cisco	UCSB-B480-M5-U	8

6.7 Servers Inventory – IT - SDC (to be covered under AMC from 6-Jan-2027 onwards)

Sr. No	Device	Make	Model Name	Specifications	Count
1	Rack Servers	HP	HP Proliant DL380 Gen10	2 * 2.1 GHz, 20 Core, CPU 512 GB RAM 2 * 1920 Gb HDD	8

6.8 Servers Inventory – IT - SDC (to be covered under AMC from 2-Feb-2027 onwards)

Sr. No	Device	Make	Model Name	Specifications	Count
1	Rack Servers	HP	HP Proliant DL380 Gen10	2 * 2.1 GHz, 20 Core, CPU 512 GB RAM 2 * 1920 Gb HDD	1

6.9 Storage Inventory – IT - SDC (to be covered under AMC from 31-Jan-2027 onwards)

Sr. No	Device	Make	Model Name	Specifications	Count
1	Storage	HP	HPE MSA 2060	5 * 20000 Gb, SSD 12 * 14000 Gb, SAS	1

6.10 Software Inventory – IT - SDC (to be covered under AMC from 6-Jan-2027 onwards)

Sr. No	Description	Make	Quantity
1	Microsoft Server Standard 2019 (Windows standard License)	Microsoft	9

Expansion BOM
6.11 New BOM for extended SDC space – Hardware

S. No	Description	Segment	Qty
1.	Firewall with 10G ports & Lic	IT	2
2.	IPS with 10G ports & lic	IT	2

3.	Access Switch 48 ports (24-Port's eth, 24-Ports FC)	IT	6
4.	Server Load Balancer	IT	2
5.	Out of band Switch (24 port)	IT	6
6.	Blade Servers (including chassis, controllers, cables and all accessories & modules etc)	IT	1000 Cores, & 6TB RAM
7.	Database Server	IT	
8.	500 TB Usable space for Proposed Storage (This additional usable space is for the storage proposed in replacement of existing storages mentioned at point 9 and 10 of RFP Vol I, 14. Annexure 4 - Inventory & Expansion BOM, Existing BoM, 6.1 Exiting Hardware Inventory – IT (SDC)). With the following Disk configuration - 30% Flash/SSD, 30% SAS, 40% NL SAS. Along with the required enclosure.	IT	500 TB usable space
9.	Advance Persistence Threat Solution (Anti - APT)	IT	2
10.	DDoS solution	IT	2
11.	Desktops	IT	4 set
12.	Data cabling for complete DC including NOC, BMS, Non-IT etc.	Non-IT	As required
13.	Fibre Cables (5 Meters, 10 Meters, 30 Meters)	Non-IT	210 (70 qty each)
14.	Access Control Solution (for DC area, UPS & Electrical room)	NonIT	1 Set
15.	Air-condition for 300 sqft except DC area 2 Tr (2+1) including accessories, intelligent timer & Stabilizer	NonIT	3
16.	Building Management System (BMS Solution) along with necessary hardware & software including Temp & RH sensors, cabling, perpetual full use processor licenses	NonIT	1 set
17.	CCTV Solution (with min 9 Dome Cameras, 2 bullet (outdoor) cameras)	NonIT	1 set
18.	LED Display	Non-IT	4 set
19.	Civil & Interior Work Including: • Brick work • Cement Concrete Work • Cutting and chipping of existing floors • Masonry works • Hardware and Metals • Glazing • False Flooring • False Ceiling • Partitioning • Doors and Locking • Painting • Fireproofing all surfaces • Water proofing • Insulating • Cold aisle containment in existing as well as expansion area • Removal of backroom wall in existing NOC room & and construction of three seats (including 3 Nos Chairs & table) • Exit path from Ground floor UPS room to 1st floor & DG platform • Exit door including panic bar • Structure for PAC ODU	NonIT	Lump sum As Required
20.	Electric Work including:	NonIT	Lump sum As Required

S. No	Description		Qty
	• Electrical cabling (SDC are including all utility components and UPS) Earthing, Lighting & Fixtures, Motion detectors, Main Electrical Panel (min 630 Amp) including its electrical cabling • Cabling upgradation/additional cabling from Transformer room to SDC Electrical panel • Cabling upgradation/additional cabling from DG Sets to SDC Electrical panel • Any other components required		
21.	Fire Extinguishers (C type)	NonIT	7
22.	Floor PDU (180 KVA) with isolation transformer - shall be used for power distribution inside the data centre	NonIT	2
23.	GAS Suppression & Fire Detection System (min 4 NOVEC 1230 cylinders - 3 Server farm area & 1 UPS room)	NonIT	1 set
24.	Glow Signage-Exit (Server Farm Area -3, UPS room - 1, Exit (with light) - 1)	NonIT	5
25.	HSSD Solution (VESDA)	NonIT	1
26.	IPDU for New Racks	NonIT	52
27.	IPKVM with LCD Monitor	NonIT	4
28.	Phase sequencer (3 Phase)-600KVA	NonIT	1
29.	Lighting (4 Nos) & CAC (3 Nos of 1.8Tr) including stabilizers for Transformer room	NonIT	1 Set
30.	Precision AC with accessories N+1 set (Working Unit - 7 Nos. of 6.8 Tr and Standby Unit - 2 Nos. of 6.8Tr) including one water purifier for water inlet supply for PAC	NonIT	9
31.	Rodent Repellent System (DC Area & UPS Room)	NonIT	2
32.	Network Racks (including blankers) Floor Standing 19" 42U 800(mm) (W)X 1000(mm)	NonIT	2
33.	Server Racks (including blankers) Floor Standing 19" 42U 600(mm) (W) X 1000 (mm)	NonIT	19
34.	UPS for BMS (5 KVA) (N=1) N+1 including battery bank	NonIT	2
35.	UPS for Expansion to 180 KVA (N=1) N+N Set - (including 2 x 240 nos batteries, 2 Volts, 300AH, Sealed Valve-Regulated lead acid (VRLA) heavy duty type batteries) scalable to 240 KVA	NonIT	2
36.	Water leak detection system (DC Area)	NonIT	2
37.	Upgradation of existing DG Set to 400 KVA x 3 (including Sync Panel) (existing Sync panel, 200 KVA x 3 Nos of DGSETs, Sanjay Diesel)	NonIT	3
38.	Tape Cartridge LTO8 with Barcode label	IT	250 qty
39.	Cisco Nexus 7018 Line Card with 12x40G uplink port (fully populated), with necessary license (if required)	IT	4

6.12 New Expansion BOM – Software (Including supply, installation, commissioning and operationalization)

S. No	Description	Qty
1.	Microsoft Windows Server Datacenter latest edition	400 cores
2.	RHEL VDC with smart management console (the licenses shall be provided to cover 600 cores, SI to make appropriate calculation based on the type of server and processor being supplied)	600 cores
3.	Microsoft SQL Enterprise edition	40 cores
4.	Device CAL License for Microsoft OS	100

S. No	Description	Qty
5.	Virtualization & unified management (the licenses shall be provided to cover 1000 cores, SI to make appropriate calculation based on the type of server and processor being supplied)	1 Lot
6.	Additional Lic of Trend Micro- Apex one - (Existing software)	150
7.	Additional Lic of Trend Micro-Deep Security Complete Protection - (Existing software)	100
8.	Additional Lic for MicroFocus EMS - SiS Pre Ed 1 OSI Migration SW E-LTU(H7W94AAE) - (Existing software)	200
9.	Additional Lic for MicroFocus EMS - Ops Brdge Rep Ad 50 OBR Nds SW E-LTU(TJ756AAE) - (Existing software)	1
10.	Additional Lic for MicroFocus EMS - Network Node Manager i Ultimate Edition 50 Node Pack for 50+ Nodes Software E-LTU (A7Z73AAE) - (Existing software)	1
11.	Additional Lic for MicroFocus EMS - Network Node Manager i Points iSPI 100 Point Pack for 100 or more Points to NNMi Ultimate Edition for Migration Software E-LTU (A8A65AAE) - (Existing software)	1
12.	Additional Lic for MicroFocus EMS - Operations OS Inst Adv SW E-LTU (TB056AAE) - (Existing software)	60

For inventory of other projects, O&M of hardware and System Software (OS and virtualization etc) including updates and upgrades, backup to and restore from Tapes will be the responsibility of DCO. However, O&M of the Departmental Application and Database would be the responsibility of concerned user Department.

Scalability BOM
6.13 Add on items

S.No	Components	Qty
1	**NON-IT Infrastructure**	
1.1	Server Rack	1
1.2	Network Rack	1
1.3	Rack PDU	1
1.4	1 module for new proposed modular UPS along with battery bankfor 15 min backup	1
2	**IT Infrastructure**	
2.1	Blade Server as per specification given in RFP	1
2.2	Blade Servers	
a.	RAM (256 GB per blade)	1
b.	CPU (CPU for blades)	1
c.	Blade Chassis (with all necessary components)	1
2.3	DB Server	
a.	RAM (256 GB)	1
b.	RAM (512 GB)	1
c.	CPU (for DB server)	1
2.3	Storage	
a.	Controller with 8 x 32Gbps Fiber Channel ports	1
b.	Controller with 4 x 25Gbps/10 Gbps ISCSI ports.	1
c.	Controller with 8 x 32Gbps Fiber Channel ports, 4 x 25Gbps/10Gbps ISCSI ports.	1
d.	256 GB global Cache	1

e.	Additional back-end ports to achieve 96 Gbps more bandwidth	1
f.	Flash/SSD (for 30 TB usable capacity. Per drive cost x number of drives to be provided)	1
g.	SAS Drive (for 30 TB usable capacity. Per drive cost x number of drives to be provided)	1
h.	NL SAS Drive (for 40 TB usable capacity. Per drive cost x number of drives to be provided)	1
i.	Enclosure for Drives (for additional 100 TB Capacity)	As required
j.	SAN Switch ports 8 ports for proposed switch with 16 Gbps FC configuration	1
k.	SAN Switch Licensing for proposed switch for 8 ports	1
l.	Cascading License for proposed switch (to meet scalability asked)	As Required
2.4	Core Switch	
a.	10g slot with necessary Lic	4
b.	10G SFP+ uplink Port	48
b.	1G UTP ports Uplink port	48
2.4	Backup	
a.	Backup licenses per DB and OS	1
2.5	Other Licenses	
a.	OS License Microsoft Windows Datacenter edition	1
b.	OS License Microsoft Windows Standard	1
C	OS License - Redhat	1
b.	DB License (MS SQL EE)	1
C	Active-Active Clustering Software License (MS SQL Enterprise Edition) with perpetual license processor based full use for Database Server	1
d.	Antivirus License	1
e.	HIPS License	1
H	EMS Server Monitoring (future scalability)	1
	EMS Network Monitoring	1
	EMS Other Modules	1
I	Directory Services - Microsoft Windows Server Enterprise Edition Latest Version CAL and with five years of updates & upgrades	1
2.6	FC Module for existing SAN Switch, fully populated 8/16 Gbps ports with SFP's	1
2.7	Any other Suggested Equipment	

Bidder to add cost for all items which are going to be EOSL during the currency of the contract and which need to be replaced or upgraded

To, _____

_____

_____

Sub: RFP Ref No.

Dear Sir,

(Authorization to be taken from Hardware/Software OEM's)

Please refer to your Notice Inviting Tenders for Appointment of an Agency for Operations & Maintenance and expansion of physical and IT infrastructure for _____ Data Center at _____

M/S _____(Bidder), who is our reliable distributor for the last _____years, is hereby authorised to quote on our behalf for this prestigious tender.M/S _____ _____(Bidder) is likely to continue as our business partner during years to come. We undertake the following regarding the supply of all the equipments and relatedsoftware as described in this tender

1. Authorization for M/S_____(Bidder) to sell the hardware / software.

2. Confirm that the products quoted are not "end of life or end of sale products" as on Bid Submission date. If in case the support for the product quoted has been stopped/ withdrawn till the time of deliveryof equipment, the same will be changed with the equivalent or superior product at no extra cost.

3. Undertake that the support including spares, patches, and upgrades for the quoted products shall beavailable for 7 years from the signing of contract or 6 years from the FAT.

Yours faithfully,

(NAME) (Name of manufacturers)

Declaration Regarding Clean Track Record

To,

_____

_____

_____

Sub: RFP Ref No.

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP Document[No. _____] regarding Appointment of a DCO for Operation & Maintenance and Expansion of the HP State Data Centre for a period of five years. I hereby declare that my company has not been debarred/black listed by any Government / Semi Government organizations in India. I further certify that I am competent officer in my company to make this declaration.

Yours faithfully,

Declaration of Acceptance of Terms and Conditions in EOI

To,

_____

_____

_____

Sub: RFP Ref No.

Dear Sir,

  I have carefully gone through the Terms & Conditions contained in the RFP document [No. ………………………………..] regarding Appointment of a DCO for Operations & Maintenance and Expansion of physical and IT infrastructure for State Data Centre.

  I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

Annexure- VI

To,

_____

_____

Ref: Tender no. ………………………………… dated …………………….

Dear Sir,

Having examined the EoI/RFP/Tender document, we hereby submit our bid for the subject requirement which has emerged from some Government body to implement the above captioned project.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to ITI Limited is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the Buyer in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the short-listing process, we are liable to be dismissed from the selection process or termination of the agreement during the project, if selected to do so.

We agree for unconditional acceptance of all the terms and conditions set out in the EoI/RFP/Tender document including annexures and corrigendum if any and also agree to abide by this tender response for a period of 6 months from the date fixed for bid opening.

We hereby declare that in case the agreement is awarded to us, we shall submit the Performance Guarantee in the form of bank guarantee in the format to be provided by ITI Limited.

We agree that ITI Limited is not bound to accept any tender response that they may receive. We also agree that ITI Limited reserves the right in absolute sense to reject all or any of the services specified in the tender response.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this

connection.

We understand that it will be the responsibility of our organization to keep ITI Limited informed of any changes in respect of authorized person and we fully understand that ITI Limited shall not be responsible for non-receipt or non-delivery of any communication and/or any missing communication in the event reasonable prior notice of any change in the authorized person of the company is not provided to ITI Limited.

Dated this   Day of   **2022**

Authorized Signatory

Name:
Designation:
(Company Seal)
Note: To be submitted in Company Letterhead

Bidder's Profile

1.	Name and address of the company			
2.	Contact Details of the Bidder (Contact person name with Designation, Telephone Number, FAX, E- mail and Web site)			
3.	Area of Business			
4.	Annual Turnover in last 3 financial years (Rs in Crore)	2019-20	2020-21	2021-22
5.	IT Turnover in last 3 financial years (Rs in Crore)	2019-20	2020-21	2021-22
6.	Profit / Loss in last 3 financial years (Rs in Crore)	2019-20	2020-21	2021-22
7.	Net-worth in last 3 financial years (Rs in Crore)	2019-20	2020-21	2021-22
8.	Date of Incorporation			
9.	GST Registration number			
10.	PAN Number			
11.	CIN Number, if applicable			
12.	Number of technical manpower in company's rolls			

Dated this   Day of   **2022**

Authorized Signatory

Name:
Designation:
(Company Seal)
Note: To be submitted in Company Letterhead

Annexure- VIII

To
ITI Limited, MSP-Delhi
Rohit House, 3 Tolstoy Marg NewDelhi-
110001

Subject: Undertaking towards Non-Black Listing of our firm by any Govt. Body

Dear Sir,

We hereby declare that we have not been BLACK LISTED by any Govt. department/ PSU (State or Central)/ Autonomous Institution against our performance obligation in India and there has been no litigation with any government department on account of similar services for the last 5 years.

This declaration is being submitted as per the requirement of your EoI/RFP/Tender.

Dated this   Day of   **2022**

Authorized Signatory

Name:
Designation:
(Company Seal)
Note: To be submitted in+ Company Letterhead

To
ITI Limited, MSP-Delhi
Rohit House, 3
Tolstoy Marg New
Delhi- 110001

Subject: Declarations against Expression of Interest (EoI) for SELECTION OF SYSTEM INTEGRATOR FOR OPERATION AND MAINTENANCE AND EXPANSION OF PHYSICAL AND IT INFRASTRUCTURE

Tender no. ……………………………... dated …………………

Dear Sir,

We hereby declare / undertake the following.

We hereby declare that we will work with ITI as per EOI/RFP/Tender terms and conditions of ITI as well as end customer including warranty & post-warranty services and implementation of the project in the event of ITI winning the contract on back-to-back basis.

We hereby declare that we will submit the Tender Fee & EMD (while submitting the bid to the end customer in the form of Bank Guarantee / Demand Draft / Online Payment from any Nationalized / Scheduled Bank) & Performance Bank Guarantee to end customer or ITI (as decided by ITI) as per EoI/RFP/Tender terms & conditions. We also undertake that we will provide EMD & PBG to ITI as per the end-customer's EoI/RFP/Tender terms even if ITI is exempted to submit the same to end- customer because of its PSU status.

We hereby declare that we have 'No Objection/ No Claim/ No Compensation' from ITI Limited if this EoI/RFP/Tender is cancelled at any stage of evaluation process by ITI or the main EoI/RFP/Tender is cancelled by the end customer.

We hereby undertake that we will be equipped with the required manpower with qualifications, certifications and experience as required in the end customer's EoI/RFP/Tender.

We hereby undertake that we will be able to give the proposed solution as required in the end customer's EoI/RFP/Tender.

We hereby undertake that we will arrange required certificate & support (warranty & post-warranty/maintenance) in the name of ITI Limited from the OEM as per end customer's requirement.

We hereby undertake that we will obtain relevant statutory licenses for operational activities.

We hereby undertake that we will sign Consortium Agreement /Teaming Agreement / Integrity Pact with ITI for addressing the end customer's EoI/RFP/Tender if required.

We indemnify ITI Limited from any claims / penalties / statuary charges / liquidated damages / legal expenses if any etc. as charged by the end customer.

We hereby undertake to make arrangement for signing of agreement between OEM and ITI as per end customer's EoI/RFP/Tender requirements.

\

We hereby undertake that the OEMs who meet the eligibility and other conditions as per end customer's EoI/RFP/Tender requirement will be finalized by us and produce the required eligibility documents and other related documents of the OEM for final bid submission.

We hereby agree to take the responsibilities covered in the agreement (on back-to-back basis) to be signed between ITI & OEM (if required) as per end customer's EoI/RFP/Tender terms&conditions.

We hereby declare to supply equipment/components which are brand new, first hand and contain no previously used, recycled or refurbished components.

We hereby declare not to partner with any other organization for addressing this EoI/RFP/Tender.

We hereby declare to accept payment terms on back-to-back basis. Penalties, if any, will be borne by us.

We hereby declare to provide Bank Guarantee (110% of value for the period till the advance is settled) forgetting the advance payment if any on back-to-back basis.

We hereby agree that ITI may take any punitive action as deemed fit, including forfeiture of EMD / Securitysubmitted by us, if it is found that any of the documents / information provided by us (to meet the tender requirement including eligibility) is wrong/ forged/ misleading at any stage of tender processing / evaluation. The decision of ITI regarding forfeiture of the EMD shall be final and shall not be called uponquestion under any circumstances

Dated this Day of   **2022**

Authorized Signatory

Name:
Designation:
(Company Seal)
Note: To be submitted in Company Letterhead

\

Annexure X

Compliance Statement of Eligibility Criteria
Ref: Tender no. ………………………….……. dated …………………..

Sl. No.	Clause No.	Clause	Compliance (Complied/Not Complied)	Remarks with Documentary Reference

Dated this   Day of   **2022**

Authorized Signatory

Name:
Design
ation:
(Comp
any
Seal)

Annexure- XI

Eligibility Criteria Check List

S. No.	Description	Submitted (Y/ N)	Page No.
	o Bid covering Letter on the Letter-Head of the Bidder Company indicating Name and Address ofthe Authorized Signatory (with Contact telephone numbers and email ID)as per Annexure- A.		
	o Signed tender document along with signed technical documents.		
	o Bidder's Profile.		
	o Proof of Empanelment with ITI (If Empaneled) or board of resolution		
	o Case–Specific Power of Attorney authorizing the bidder to submit the Bid/EoI on behalf of the Bidder/Consortium.		
	o Tender-Document Cost (if any) of required amount.		
	o Copy of PAN Card.		
	o Insolvency certificate		
	o Detailed Methodology and technical work		
	o GST Registration Certificate.		
	o Turnover Certificate(s)/Audited Balance-sheet(s) & Profit-Loss Account(s) of the Bidder for last three years.		
	o Declaration on the Letter-Head of the Bidder Company for Non-Black Listing		
	o Declaration / Undertaking on the Letter-Head of the Bidder Company as per Annexure(s).		
	o Compliance Statement of 'Eligibility Criteria of the Bidder' along with supporting documents (credentials, experience certificates, declarations & others)		
	o Integrity Pact		
	o Tender Documents duly signed & accepted by the bidder		
	o Technical Solution		
	o Technical Presentation		
	o MAF and other undertakings from OEM		
	o Tender Fee Proof		
	o EMD Proof		
	o Work Order/ Completion Certificate as per eligibility		